Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 22 *Volume XXII*
Number 3 *Volume XXII Book 3*

Article 2

2012

# The Future of Cybertravel: Legal Implications of the Evasion of Geolocation

Marketa Trimble
*William S. Boyd School of Law, University of Nevada, Las Vegas*, marketa.trimble@unlv.edu

# The Future of Cybertravel: Legal Implications of the Evasion of Geolocation

## Cover Page Footnote

Associate Professor of Law, William S. Boyd School of Law, University of Nevada, Las Vegas. The author thanks her colleagues at the William S. Boyd School of Law for their comments and suggestions, particularly Professor Mary LaFrance, Professor Ann McGinley, Professor Francis J. Mootz III, and Professor Jean Sternlight. She would also like to thank Professor Pedro de Miguel Asensio, Professor Derek Bambauer, Professor Adam Candeub, Professor John Cross, JUDr. Adela Faladova, Paul Geller, Professor Eric Goldman, Professor Paul Goldstein, Professor Thomas Hoeren, Professor Paul C. Van Oorschot, Professor David G. Post, Wendy Seltzer, Professor Brenda Simon, and Professor Dan Jerker B. Svantesson. The author appreciates the helpful input from the participants of the 2011 Internet Law Works in Progress conference, the 2011 Intellectual Property Scholars Conference, and the 39th Research Conference on Communication, Information and Internet Policy. The author is indebted to David McClure and Jennifer Anderson at the Wiener-Rogers Law Library of the University of Nevada, Las Vegas, and Shweta Kadam of the William S. Boyd School of Law for valuable research support, and Ammon Francom and William “Hunter" Campbell, J.D. candidates at the William S. Boyd School of Law. The author thanks Gary A. Trimble for his unlimited support for her research and writing. Finally, the author would like to recognize a friend from Sunnyvale, California, who inspired the author to write this article.

# The Future of Cybertravel: Legal Implications of the Evasion of Geolocation

Marketa Trimble*

*Although the Internet is valued by many of its supporters particularly because it both defies and defeats physical borders, these important attributes are now being exposed to attempts by both governments and private entities to impose territorial limits through blocking or permitting access to content by Internet users based on their geographical location—a territorial partitioning of the Internet. One of these attempts is the recent Stop Online Piracy Act ("SOPA") proposal in the United States. This article, as opposed to earlier literature on the topic discussing the possible virtues and methods of erecting borders in cyberspace, focuses on*

* Associate Professor of Law, William S. Boyd School of Law, University of Nevada, Las Vegas. The author thanks her colleagues at the William S. Boyd School of Law for their comments and suggestions, particularly Professor Mary LaFrance, Professor Ann McGinley, Professor Francis J. Mootz III, and Professor Jean Sternlight. She would also like to thank Professor Pedro de Miguel Asensio, Professor Derek Bambauer, Professor Adam Candeub, Professor John Cross, JUDr. Adela Faladova, Paul Geller, Professor Eric Goldman, Professor Paul Goldstein, Professor Thomas Hoeren, Professor Paul C. Van Oorschot, Professor David G. Post, Wendy Seltzer, Professor Brenda Simon, and Professor Dan Jerker B. Svantesson. The author appreciates the helpful input from the participants of the 2011 Internet Law Works in Progress conference, the 2011 Intellectual Property Scholars Conference, and the 39th Research Conference on Communication, Information and Internet Policy. The author is indebted to David McClure and Jennifer Anderson at the Wiener-Rogers Law Library of the University of Nevada, Las Vegas, and Shweta Kadam of the William S. Boyd School of Law for valuable research support, and Ammon Francom and William "Hunter" Campbell, J.D. candidates at the William S. Boyd School of Law. The author thanks Gary A. Trimble for his unlimited support for her research and writing. Finally, the author would like to recognize a friend from Sunnyvale, California, who inspired the author to write this article.

*an Internet activity that is designed to bypass the territorial partitioning of cyberspace and render any partitioning attempts ineffective. The activity—cybertravel, or the evasion of geolocation—permits users to access content on the Internet that is normally not available when they connect to the Internet from their geographical location. By utilizing an Internet protocol address that does not correspond to their physical location, but to a location from which access to the content is permitted, users can view or use content that is otherwise unavailable to them. Although cybertravel is not novel (some cybertravel tools have been available for a number of years), recently the tools allowing it have proliferated and become sufficiently user-friendly to allow even average Internet users to utilize them. Indeed, there is an increasing interest in cybertravel among the general Internet public as more and more website operators employ geolocation tools to limit access to content on their websites from certain countries or regions.*

*This article analyzes the current legal status of cybertravel and explores how the law may treat cybertravel in the future. The analysis of the current legal framework covers copyright as well as other legal doctrines and the laws of multiple countries, with a special emphasis on U.S. law. The future of the legal status of cybertravel will be strongly affected by the desire of countries and many Internet actors to erect borders on the Internet to facilitate compliance with territorially-defined regulation and enjoy the advantages of a territorially-partitioned cyberspace. This article makes an attempt to identify arguments for making or keeping certain types of cybertravel legal, and suggests legal, technological, and business solutions for any cybertravel that may be permitted.*

## INTRODUCTION

An important decision awaits countries and the international community at large: whether people should be free to break the territorial limits that governments and other entities attempt to impose on the Internet—whether Internet users should have the freedom to travel in cyberspace. Traveling in cyberspace, or "cybertravel," allows Internet users to view the Internet as if they were in a location other than where they are physically present. Users cybertravel by altering the information that identifies the geographical location from which they are accessing the Internet on the device they use to connect to the Internet. Once they alter the information, they appear to the Internet world to be physically located in a different location. Through cybertravel, Internet users are able to view or use content on the Internet that they would otherwise not be permitted to access because of geolocation tools that block access to content based on the geographical location of a user.

While cybertravel is a network capability that many users appreciate, it frustrates the efforts of those who want geographical borders to be created and maintained on the Internet so that

Internet actors[1] can comply with territorially-defined regulations or contractual obligations and enjoy certain advantages that result from a territorially-partitioned cyberspace—for example, the possibility of price differentiation in different markets or localized advertising. Whether cybertravel should or should not be legal is not a matter of abstract academic debate; it is an important question that has already appeared on legislative agendas.[2] This article presents cybertravel and its forms, explains the various uses of cybertravel, and assesses its legality. It discusses whether there is a place for legal cybertravel on the Internet, and if there is a place, what legal, technological, and business solutions may facilitate that cybertravel. Current developments make the discussion of the legality of cybertravel particularly timely; because cybertravel could subvert these developments, it is important at this point to clarify what its status should be.

There is evidence of an increasing interest in the territorial partitioning of the Internet. Despite the various projections for the future of the Internet that predicted a specific type of regulation that would apply to and on a "borderless medium,"[3] governments want to have the territorial scope of regulation and enforcement on the Internet mirror the territorial limits of the physical world.[4] This governmental interest in borders on the Internet is shared by private parties; while governments seek ways to protect their

---

1 The term "Internet actors" is used not only to describe Internet users but also to describe anyone who acts on the Internet: website operators, Internet service providers, etc. For an explanation of the terms "website operator" and "Internet service provider" as used in this article see *infra* notes 6 and 61 and the accompanying text.

2 *See* Stop Online Piracy Act, H.R. 3261, 112th Cong., § 102(c)(4)(A)(ii) (2011).

3 *See infra* Part I. A difference may be drawn between the regulation of the medium (regulation *of* the Internet—e.g., who should be in charge of assigning addresses on the Internet) and the regulation of activities that occur on the medium (regulation *on* the Internet—e.g., consumer protection laws, tax laws, defamation laws that apply to conduct on the Internet). This article concerns any national regulation that is limited to a certain territory; such national regulation includes both types of regulation—regulation *of* the Internet (e.g., rules for Internet service providers) and regulation *on* the Internet (all national laws that may pertain to conduct on the Internet).

4 *See* Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 785 (2001).

citizens from the influx of certain content,[5] website operators[6] search for workable solutions to partition cyberspace in order to both secure compliance with territorially-limited regulation and enforcement and take advantage of the partitioned cybermarket. To achieve the partitioning, entities on the Internet employ geolocation tools to localize Internet users and control the content that is available to the users based on their location. Increasingly, geolocation is not only a matter of voluntary adoption by Internet actors but also a matter of decree: governments and courts are beginning to mandate the use of geolocation tools as a valid means of achieving compliance with the laws of particular jurisdictions.[7] It is likely that as geolocation use increases to limit access to certain content[8] it will generate more interest in cybertravel,[9] which will become widespread, undermine geolocation efforts, and

[5] *See, e.g.*, *infra* note 56 (seizures of domain names in the United States); *see also Country Profiles*, OPENNET INITIATIVE, http://opennet.net/country-profiles (last visited Mar. 7, 2012) (numerous examples of countries ordering Internet service providers to block certain websites). For the term "Internet service provider" as used in this article *see infra* note 61 and the accompanying text.

[6] The term "website operator" describes any entity that runs its own website. This term is to be distinguished from "Internet service provider." *See infra* note 61 and accompanying text.

[7] *See infra* notes 86–89 and accompanying text.

[8] The 2010 Internet-Draft of the Geographic Location/Privacy (geopriv) group of the Internet Engineering Task Force has noted that "[a]s the accuracy of location information improves and the expense of calculating and obtaining it declines, the distribution and use of location information in Internet-based services will likely become increasingly pervasive." Barnes et al., *An Architecture for Location and Location Privacy in Internet Applications: Internet-Draft*, GEOPRIV4 (Oct. 11, 2010), http://tools.ietf.org/pdf/draft-ietf-geopriv-arch-03.pdf; *see also* A. Mayrhofer & C. Spanring, *A Uniform Resource Identifier for Geographic Locations ('geo' URI)*, INTERNET ENG'G TASK FORCE 4, (June 2010), http://www.rfc-editor.org/rfc/pdfrfc/rfc5870.txt.pdf ("Most web search engines use geographic information, and a vivid open source mapping community has brought an enormous momentum into location aware technology.").

[9] *See* Benjamin Edelman, *Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-Air Television Content to Canadian Internet Users* 9 (2001), *available at* http://cyber.law.harvard.edu/archived_ content/people/edelman/pubs/jump-091701.pdf (expert memorandum attached to the National Association of Broadcasters' submission to Industry Canada) ("The availability of exclusive high-value content protected by geographic analysis systems would be likely to encourage additional efforts at circumvention via proxy servers.").

make territorially-limited regulation and enforcement on the Internet even more difficult.

The seminal question for regulating the use of cybertravel is whether it should be allowed at all, considering its potential to severely undermine the current trajectory of regulation and enforcement on the Internet. The most straightforward manner of addressing the potentially subversive effect of cybertravel is to make it illegal. Absent cybertravel, geolocation tools would face minimal or negligible obstacles and national regulation and enforcement on the Internet could emulate that of the physical world.

This article supports the survival of cybertravel with specific limitations. It argues that cybertravel should be equated to physical travel, and advocates that the legality of cybertravel should be protected for the same reasons for which we value the freedom of physical travel. The importance of physical travel, including international travel, which in the United States is underscored by constitutional protections,[10] emanates from its benefits to society, not the least of which is the access to information about alternative views and practices.[11] People who travel learn about views held by others and various solutions to social problems, regulation, and enforcement. Travel can inspire, teach, and facilitate an understanding of other societies, and assist in securing a peaceful co-existence of nations.[12] In the near future, cybertravel will play a role very similar to that of physical travel as cyberspace becomes as partitioned as the physical world. Even if this partitioning is the result of the imposition of reasonable jurisdictional limits on the Internet, it is questionable whether the resulting borders should be less permeable than the borders of the physical world.

---

[10] Kent v. Dulles, 357 U.S. 116, 125 (1958); *see infra* Part IV.B.3.

[11] *Id.* at 125–27 (quoting ZECHARIAH CHAFEE, THREE HUMAN RIGHTS IN THE CONSTITUTION OF 1787 195–96 (University of Kansas Press 1956)). On the right to access to information, see *infra* Part IV.B.3.

[12] *Id.* at 127 (quoting ZECHARIAH CHAFEE, THREE HUMAN RIGHTS IN THE CONSTITUTION OF 1787 195–96 (University of Kansas Press 1956)).

This article analyzes cybertravel and its current status, and projects its future. Part I discusses the notion of the "borderlessness" of the Internet, its origins, development, and current state. Part II discusses one of the methods used today to defeat Internet borderlessness and allow the erection of borders; the method—arguably the preferred of the existing methods of the territorial partitioning of the Internet[13]—relies on geolocation tools to partition cyberspace. Part II explains how geolocation tools work, who uses them and for what purposes. Part III focuses on the use of cybertravel as the evasion of geolocation. It reviews the various methods of cybertravel and provides examples of its uses. Part IV analyzes the legality of cybertravel as it exists today and proposes approaches that the law could take to cybertravel in the future; it also discusses possible technological and business solutions that may make cybertravel possible notwithstanding the developments that appear to preordain cybertravel's illegality.

It should be noted that two topics are peripheral to the primary focus of this article.[14] Although the article touches upon the two topics—anonymization and place-shifting services—they are not its primary focus. Although it may appear that the problem of achieving anonymity on the Internet (or anonymous Internet browsing) is related to the legal issues of cybertravel, anonymization is in fact neither a prerequisite for nor a consequence of the legalization of cybertravel. The relationship between the two phenomena is analyzed in Part IV,[15] but this article provides no answers to questions about anonymization. Place-shifting services, which either retransmit television programs

[13] Another method of erecting borders on the Internet is the filtering imposed by Internet service providers. Internet service provider filtering prevents users from accessing content that has been blocked by the provider. The most controversial method consists of installing a filter on users' hardware. *See infra* Part I (discussing methods of erecting borders on the Internet). For the definition of "Internet service provider" as used in this article, see *infra* note 61 and accompanying text.

[14] In attempting to cover a broad scope of various legal issues that pertain to cybertravel, this article inevitably generalizes and omits in-depth analyses of some issues deserving separate detailed inquiries (e.g., issues of personal jurisdiction and the legal status of *cache* copies). Such inquiries are beyond the scope of this article.

[15] On the relationship (or the absence thereof) of anonymization and cybertravel see *infra* Part IV.B.2.

themselves (e.g., ivi in the United States,[16] TV CatchUP in the United Kingdom,[17] shiftTV in Germany,[18] and ManekiTV in Japan),[19] or enable users to share retransmission of television programs (e.g., Justin.tv[20] and WorldTV),[21] resemble cybertravel because they also secure access to content in places where the content is normally not available.[22] Although recent legal disputes concerning these services[23] may be the precursors to legal challenges to cybertravel, legal issues that concern place-shifting services do not coincide with but only overlap with the issues associated with cybertravel.[24]

---

16 IVI, http://www.ivi.tv/faq (last visited Nov. 19, 2011).

17 TVCATCHUP, http://www.tvcatchup.com (last visited Nov. 19, 2011).

18 SHIFTTV, http://www.shift.tv (last visited Nov. 19, 2011).

19 MANEKITV, http://www.manekitv.com (last visited Nov. 19, 2011).

20 JUSTIN.TV, http://www.justin.tv (last visited Nov. 19, 2011). According to its CEO, Michael Seibel, Justin.tv "provide[s] a platform that empowers people to create and share live video online. Our site is the modern equivalent of the town square, but instead of standing on a soap box to be heard a user can broadcast his or her message to the world." *Piracy of Live Sports Broadcasting over the Internet*: Hearing before the Comm. on the Judiciary, 111th Cong. 25 (2009) (Statement of Michael Seibel, CEO, Justin.tv, Inc.).

21 WORLDTV, http://worldtv.com/pages (last visited Nov. 19, 2011).

22 For a reference to Slingbox, another non-cybertravel service that offers access to territorially-limited content, see *infra* note 259.

23 *See, e.g.*, WPIX, Inc. v. Ivi, Inc., 765 F. Supp. 2d 594 (S.D.N.Y. 2011); Toshiko Aritake, *Top Court Says Retransmission of Network TV Content Violates Copyrights*, 25 WORLD INTELL. PROP. REP. (BNA) 16 (Jan. 25, 2011); ITV Broad. Ltd. v. TV CatchUp Ltd., [2010] EWHC (Ch) 3063; ITV Broad. Ltd. v. TV CatchUp Ltd., [2011] EWHC (Pat) 1874; and ITV Broad. Ltd. v. TV CatchUp Ltd., [2011] EWHC (Pat) 2977; Bundesgerichtshof, [BGH] [Federal Court of Justice], Apr. 22, 2009, MEDIEN, INTERNET UND RECHT [MIR] 173, 2009 (Ger.) (*Shift.tv*). The Ultimate Fighting Championship filed a lawsuit against Justin.tv on January 21, 2011. Complaint, Zuffa, LLC v. Justin.tv, Inc., No. 2:11-cv-00114-RLH-LRL (D. Nev. filed Jan. 21, 2011). *See also Piracy of Live Sports Broadcasting over the Internet*: *Hearing before the Comm. on the Judiciary*, 111th Cong. 25 (2009) (statement of Michael Seibel, CEO, Justin.tv, Inc.); *see also infra* Part IV.A.2.

24 First, because of the manner in which the technology involved in cybertravel functions, as opposed to the manner in which place-shifting tools that are mentioned here function, cybertravel might not be viewed as a retransmission of content to a new (not originally intended) audience. Second, even if the differences in technology are considered irrelevant to an inquiry about the existence of liability for copyright infringement, not all legal issues relevant to cases of cybertravel would apply to place-shifting services. Although users do cybertravel to watch video content not available in their country or region, this is not the only purpose for which they cybertravel, and therefore limiting the present inquiry to this one aspect of cybertravel would most

## I. THE INTERNET AS A BORDERLESS MEDIUM[25]

At its birth, the Internet was endowed with an architecture that sounded very appealing: the medium would be designed so that no one authority could assert complete control over it.[26] This design idea shaped the creation of the Arpanet, the predecessor of the Internet,[27] as a decentralized network that would become the basis of the structure of the Internet. This deliberate design led to a network that not only defied central control but also lacked borders for partitioning control territorially; one of the network's defining features was the absence of any borders. Dan Jerker B. Svantesson, who has worked on the legal problems associated with the Internet's borderlessness and issues of geolocation for a number of years,[28] calls borderlessness "one of [the Internet's]

certainly not exhaust all the legal issues associated with cybertravel, and the limitation would render the legal analysis of cybertravel incomplete. *See infra* Part IV.A.2 for the discussion of various legal aspects concerning cybertravel. For the legal issues of the streaming of content on the Internet, see Maurizio Borghi, *Chasing Copyright Infringement in the Streaming Landscape*, 42 INT'L REV. INTELL. PROP. & COMP. LAW 316 (2011).

[25] The word "Internet" technically refers to only one of the network protocols; however, given the prevailing use of the protocol and the fact that it has been equated to the network itself, this paper talks only about the Internet. On the two current versions of the protocol *see infra* Part II.B.

[26] *See* JACK L. GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 23 (Oxford University Press 2006) ("[T]he founders embraced a design that distrusted centralized control. In effect, they built strains of American libertarianism, and even 1960s idealism, into the universal language of the Internet."); INSTRUCTIONAL DESIGN: SYSTEM, STRATEGIES 167 (Bruce R. Ledford, Phillip J. Sleeman, eds.) ("Primarily because of the needs inherent in the cold war, it became obvious to the Military and Department of Defense that the ability to wage modern warfare had to be decentralized."); *see also* Paul Baran, *On Distributed Communications: I. Introduction to Distributed Communications Networks*, RAND CORP. (Aug. 1964), http://www.rand.org/pubs/research_memoranda/2006/RM3420.pdf.

[27] *See generally* JANET ABBATE, INVENTING THE INTERNET (MIT Press 2000) (discussing the creation and early days of the Internet); *see also* GOLDSMITH & WU, *supra* note 26, at 22–23.

[28] Svantesson has written about geolocation since 2003. Dan Jerker B. Svantesson, *How Does the Accuracy of Geo-Location Technologies Affect the Law*, 2 MASARYK U. J. L. & T. 11, 20 (2008), *available at* http://mujlt.law.muni.cz/storage/1234798550_sb_02_svantesson.pdf [hereinafter Svantesson, *The Accuracy of Geo-Location*]. A number of Svantesson's papers related to geolocation are available on his website.

greatest attributes."[29] This Part discusses this feature of the Internet, its origins, its impact on the Internet and regulation of the Internet, and its current state and future.

Robert Taylor, a former Director of the Information Processing Techniques Office of the Advanced Research Project Agency, the agency that developed the Arpanet in the late 1960s, attributed the idea for the particular architecture of the Arpanet (that led to the borderlessness of the Internet) to Wesley Clark, an electrical engineer who worked for Washington University in St. Louis during that time. Taylor recalled that the decision to support Clark's idea was related to Taylor's own skepticism of central authority; his experience from the Vietnam War convinced him that any central authority should not be trusted, so he agreed with a plan to establish the network with no central control.[30] In fact, however, the Department of Defense also had its own reasons for being interested in a decentralized architecture; such an architecture was more likely to withstand an enemy attack.[31] Therefore, the distributed architecture of the network was not a matter of coincidence,[32] nor was it dictated by technical necessity;

SVANTESSON.ORG, http://www.svantesson.org/projects/geo-identification/articles--papers-relating-to-geo-identification.aspx (last visited Nov. 19, 2011).

[29] Dan Jerker B. Svantesson, *"Imagine There's No Countries…"—Geo-Identification, the Law, and the Not-So-Borderless Internet*, 10 J. INTERNET L. 1, 1, 20 (2007).

[30] Computer History Museum, *Net @ 40: Robert W. Taylor in Conversation with National Public Radio's Guy Raz*, YOUTUBE (May 13, 2010), http://www.youtube.com/computerhistory#p/search/0/Y0MsrrTo8jY ("Other people who were thinking about the networking architecture as we would design it were imagining central locations for a single computer in the middle of the country that would control the network all over the country. What a stupid idea! I knew it was a stupid idea but I did not have a better one. Wes[ley] Clark had a better one."). For Taylor's recollections of his experience from the Vietnam War era, see *id.*; *see also* John Markoff, *Control the Internet? A Futile Pursuit, Some Say*, N.Y. TIMES, Nov. 14, 2005, at C4, *available at* http://www.nytimes.com/2005/11/14/business/14register.html?_r=2 (discussing Taylor's recollections); *see also* Jonathan Zittrain, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 28–35 (2008) (explaining the beginnings of the Internet in general).

[31] Baran, *supra* note 26.

[32] *Cf.* DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 103 (2009) ("Perhaps it was a coincidence that the network that became 'the Internet' was the one that operated this way: end-to-end, innovations coming from the edges via this strange kind of creeping consensus among users, no centralized control. I doubt it, though.").

the particular architecture had significant political and strategic motivations.[33]

The technical design of the Internet has a critical impact on the power of governments to impose regulation and enforcement in the space.[34] To regulate a territory, a government needs to exert its enforcement power in the territory, or have other governments wield this power on its behalf. The willingness—or lack thereof—of foreign governments to lend their support to enforcing one government's regulations defines the limits of the power of that government to regulate. The problem in a borderless world is that if a government has the physical ability to enforce its will, for instance, because Internet servers are located in its territory,[35] it ultimately regulates and enforces worldwide; other governments cannot push back,[36] and the regulating and enforcing power of the one country thus extends to the world's entire cyberspace.[37] On the other hand, if a government cannot enforce its regulations because particular servers, server providers, website operators or their assets are located outside of that government's enforcement

---

[33] Computer History Museum, *supra* note 30, at 1:17:25 (noting that the fact that "the Arpanet was deliberately heavily decentralized . . . came from political motivations as well as technical motivations.").

[34] *Id.* at 1:12:21 (Taylor claims that the creators of the Arpanet realized that its borderlessness would not be limited to the United States but would extend globally. He recalls that it did not appear that "anyone who worked on [the Arpanet] in those days thought it would be limited to the United States.").

[35] The physical presence of the website operator or its assets does not have to be in the country of enforcement; servers may be targets of enforcement actions instead. *Cf.* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1217 (1998) ("A defendant's physical presence or assets within the territory remains the primary basis for a nation or state to enforce its laws.").

[36] Governments may try to build walls on the Internet that will keep certain content out of their territory; however, filtering is associated with a number of problems. The U.S. government is using its enforcement power over "related actors" (Internet service providers, payment processors, etc.) to enforce its laws, but U.S. legislative initiatives that target such related actors are not without controversy. *See infra* notes 59–65 and accompanying text.

[37] Anupam Chander, *Trade 2.0*, 34 YALE J. INT'l L. 281, 285 (2009) ("Left unattended, footloose net-work might imperil domestic laws, replacing local law with the regulation, if any, of the net-work provider's home state . . . [T]he importing of services should not require us to import law as well.").

power, that government's regulatory power is nonexistent[38] unless the government manages to exert its power over Internet users residing in its territory or other actors located in its territory. Such actors may include service providers and payment processors, or anyone that facilitates the operations of the website operators.[39]

When the Internet became a mass medium, the initial desire to have no central authority controlling the network was replaced by a realization that non-regulation in cyberspace might create more problems than the socially valuable opportunities that this architecture might offer. Some questioned whether the Internet was susceptible to any regulation at all. It is not surprising that the disadvantages of non-regulation on the Internet were identified by someone who personally observed the regulatory disarray in the post-communist countries. Lawrence Lessig, who was engaged as an advisor to these countries,[40] suggested a need for governance on the Internet and posited that the regulation should be based on the "code"—the architecture of the Internet, the technical design that de facto regulates behavior on the Internet.[41] The architecture would dictate to a large degree what the law could do, and be the "code," not only in the technical sense, but to a certain degree also in the legal sense.[42] If governments wished to regulate the Internet

---

[38] *See* Goldsmith & Sykes, *supra* note 4, at 789–90 (describing a potential hurdle to interstate enforcement within the United States associated with the lack of physical borders on the Internet and therefore with the danger of territorially-unlimited prescriptive jurisdiction).

[39] Targeting "related actors"—actors that are linked to providers of certain content—can raise concerns that are similar to those that are raised by filtering. *See infra* note 59 (describing the proposed Stop Online Piracy Act in the United States, which would target such related actors).

[40] LAWRENCE LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE 3 (Basic Books 1999).

[41] *See* Michael Geist, *Cyberlaw 2.0*, 44 B.C. L. REV. 323, 357 (2003) ("[T]he three principles of Cyberlaw 1.0 . . . are in fact tied together by one larger principle—that government would not, could not, and should not apply its traditional regulatory mechanisms to the Internet.").

[42] WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE AND THE INFOBAHN 111 (1996) (discussing the famous "code is the law"); Christoph B. Graber, *Internet Creativity, Communicative Freedom and a Constitutional Rights Theory Response to "Code is Law"*, at 5 (The Research Centre for International Communications and Art Law at the University of Lucerne, Working Paper No. 2010/03), *available at* http://ssrn.com/abstract=1737630 (correctly pointing out that Lessig "does not equalise

they would have to utilize its architecture—its "code" in the technical sense; at the same time, the architecture would protect the Internet from government imposition of laws inconsistent with the structure of the network.[43] The solution to the problem of regulation on the Internet would have to be predicated on its architecture.

If conduct on the Internet should and could be regulated, the question then was who should regulate it. One school of thought declared that no one should regulate conduct on the Internet,[44] although the "no one" did not really mean a complete absence of regulation. Because the technical "code" is a significant regulatory tool, it is clear that the "no one" would be the Internet designers, who continue to shape the Internet and its de facto technical regulatory framework.[45] Although Internet designers would always have an important role to play in the Internet's future, including the Internet's susceptibility to certain types of regulation, there seems to be no legitimate reason that they should dictate the full scope of the "code" in the legal sense.[46] Despite their "parental claims," Internet designers would not be the proper

'law' and 'code;'" rather, he "defines 'code' as a form of co-action between software and hardware on the Internet constituting an *architecture* of technology," which "is a structure that conditions regulation on the Internet.").

[43] LAWRENCE LESSIG, CODE: VERSION 2.0 3 (Basic Books 2006) ("The claim for cyberspace was not just that governments would not regulate cyberspace—it was that government *could not* regulate cyberspace.").

[44] John Perry Barlow, *Declaration of Cyberspace Independence*, ELEC. FRONTIER FOUND. (Davos, Switzerland 1996), *available at* https://projects.eff.org/ ~barlow/ Declaration-Final.html.

[45] Graber, *supra* note 42, at 5 ("[T]he actor who reigns over the architecture of technology also defines the rights and constraints existing within this architecture.").

[46] LESSIG, *supra* note 40, at 8 (There were advocates of an expert-centered approach: "We are at a stage in our history when we urgently need to make fundamental choices about values, but we should trust no institution of government to make such choices."); GOLDSMITH & WU, *supra* note 26, at 30 ("Internet's founding vision [was] of an open, noncommercial network run by selfless experts for the benefit of all."). Of course, given many people's disillusions with the choices of democratic governments perhaps it would be better to entrust regulation to independent experts; however, such an approach to shaping the "code" should have a democratic oversight unless we want to abandon democracy altogether. *See also* Graber, *supra* note 42, at 6 (discussing the need to subject to constitutional scrutiny not only governmental but also private actions manipulating Internet infrastructure).

authority to make all the regulatory choices for life in cyberspace.[47]

Those who have agreed on the need to regulate in cyberspace have been divided between those who have predicted a special new type of regulation for the Internet,[48] and those who have rejected any specificity for the medium and have insisted that the Internet be subject to the same regulations that apply to conduct occurring in other means of communication. The first group, the Internet exceptionalists, call for new bodies to be established to govern cyberspace.[49] The second group, the Internet non-exceptionalists, have seen no reason to discuss who should govern cyberspace because in their view the Internet should be subject to existing regulation.[50]

With the increasing population of cyberspace and a growing spectrum of activities taking place on the Internet, the world did not wait for a resolution of the debate among the Internet designers, the exceptionalists, and the non-exceptionalists. As Michael Geist observed in 2003, the innocent age of the Internet

---

[47] In fact, the "code" in the technical sense cannot serve as the only regulatory framework in cyberspace; there are limitations of the "code" in the technical sense and a need for it to be supported by other forms of regulation. *See* Barnes et al., *supra* note 8, at 6–7.

[48] GOLDSMITH & WU, *supra* note 26, at 25 (The options include "the internationalists' view" that "territorial rule would need to be supplemented, and eventually replaced, by global governmental institutions."). Another option is for the Internet community to govern itself independently of national governments. *See* POST, *supra* note 32, at 185 ("[I]t's all just people in one place interacting and communicating with other people in other places. So why not begin by recognizing their right–perhaps even their inalienable right?–to govern themselves as they see fit?").

[49] David R. Johnson & David G. Post, *Law and Borders–The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) ("This . . . distinct Cyberspace . . . needs and can create its own law and legal institutions.").

[50] *See* Goldsmith & Sykes, *supra* note 4, at 827 ("The error is the belief that the Internet is a unique phenomenon that requires suspension of the normal principles that govern cross-border conduct."); Goldsmith, *supra* note 35, at 1250 ("Cyberspace transactions are no different from 'real-space' transnational transactions. . . . There is no general normative argument that supports the immunization of cyberspace activities from territorial regulation. . . . Resolution of the choice-of-law problems presented by cyberspace transactions will be challenging, but no more challenging than similar problems raised in other transnational contexts."); *see also* POST, *supra* note 32, at 166–67 (discussing exceptionalists' versus non-exceptionalists' views).

was replaced by the rule of "cyberlaw 2.0," which confirmed the views and predictions of the non-exceptionalists, and "[brought] with it a shift from a borderless network to borderless law, from code that regulates to code that is regulated, and from self-regulation to government regulation."[51] History proved that the borderless network would not have to mean the end of governmental control or the end of regulation and enforcement, but that it would be transformed into a borderless regulation supported by unilateral and yet globally-reaching enforcement.[52]

Once governments began to engage in de facto global enforcement on the Internet, the borderlessness of the network no longer appeared to be an advantage, and the desirability of borders began to be re-evaluated. This development can be perceived as a logical result of the maturing of both the Internet and some of its advocates; or, a much less encouraging explanation suggests that the interest in raising borders on the Internet was one of the signs of the inevitable "Cycle" that Tim Wu has described in various industries and great inventions[53]—the "Cycle" that turns amazing, groundbreaking inventions into the tools of vicious monopolies.[54] And, counter-intuitively, raising borders may in fact assist such monopolies in asserting their power globally: while without

---

[51] Geist, *supra* note 41, at 358.

[52] *Id.* at 335–47 (Geist listed examples of "aggressive extra-territorial legislative approach" in the areas of copyright, domain names regulation, privacy, computer crime, and online gambling.); *see also* Jack Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 483 (1998) (an earlier piece by Jack Goldsmith predicting cyberlaw 2.0).

[53] TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 6 (2010) ("Without exception, the brave new technologies of the twentieth century–free use of which was originally encouraged, for the sake of further invention and individual expression–eventually evolved into privately controlled industrial behemoths, the 'old media' giants of the twenty-first, through which the flow and nature of content would be strictly controlled for reasons of commerce.").

[54] *Id.* at 7 ("If the Internet, whose present openness has become a way of life, should prove as much subject to the Cycle as every other information network before it, the practical consequences will be staggering."); *see also* GOLDSMITH & WU, *supra* note 26, at 10 ("By 2005 Yahoo had come full circle. The darling of the Internet free speech movement had become an agent of thought control for the Chinese government. . . . The Yahoo story encapsulates the Internet's transformation from a technology that resists territorial law to one that facilitates its enforcement.").

borders those who hold monopolies in only some countries face competition on the Internet from foreign competitors, with borders the monopoly holders may fully occupy the space.

Although it may seem at first that raising Internet borders is inherently undesirable, the fact is that raising borders may be as liberating as it is limiting.[55] The geographically unlimited regulation and enforcement of cyberlaw 2.0 has been liberating only when it is "our" laws that are being enforced; as soon as other countries enforce "their" laws that are contrary to our beliefs, we begin to look for ways to protect our own value system.[56] We might not always agree with our government's actions, but at least we have the option of influencing them. Having foreign governments imposing regulations on us that we cannot affect makes us reconsider the value of borders,[57] and contemplate ending the borderlessness of the Internet.[58]

---

[55] Goldsmith & Sykes, *supra* note 4, at 796–97 (discussing benefits of territorially-limited or geographically-defined regulations).

[56] GOLDSMITH & WU, *supra* note 26, at 152 ("A bordered Internet is valuable precisely because it permits people of different value systems to coexist on the same planet."). *See, e.g.*, Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001), *rev'd en banc*, 433 F.3d 1199 (9th Cir. 2006); Sarl Louis Feraud Int'l. v. Viewfinder, Inc., 489 F.3d 474 (2d Cir. 2007). *But cf. Government Domain Name Siezures Violate First Amendment*, ELEC. FRONTIER FOUND. (June 21, 2011), https://www.eff.org/press/archives/2011/06/20 (describing reactions to the seizures of domain names by the U.S. government in response to allegations of providing access to counterfeited or copyright-infringing content). According to a BNA report, between 2009 and February 2011 "[t]he government has seized nearly 100 domains." John Herzfeld, *Domains Seized by Authorities for Publishing Hyperlinks to Unauthorized Streaming Video*, BNA, Feb. 9, 2011; *see also Federal Courts Order Seizure of 150 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ, ICE HSI and FBI Cyber Monday Crackdown*, U.S. DEP'T OF JUSTICE (Nov. 28, 2011), http://www.justice.gov/opa/pr/2011/November/11-ag-1540.html (describing seizures of domain names).

[57] "[C]ontrary to what many expect, the geographically bordered Internet has many underappreciated virtues. . . . The bordered Internet accommodates real and important differences among peoples in different places, and makes the Internet a more effective and useful communication tool as a result." GOLDSMITH & WU, *supra* note 26, at viii.

[58] It also transpired that businesses did not respond to cyberlaw 2.0 by moving their seats, servers and assets to jurisdictions with limited regulation and enforcement. The absence of the feared "race to the bottom" may be explained by the global nature of large businesses for which operating against local regulations is extremely disadvantageous; they may have assets in multiple countries, which they need to protect from potential

There are three methods of imposing borders on the Internet: the first two methods rely on content filtering and the third relies on the actions of website operators.[59] Content filters can be installed directly on a user's hardware or applied at the level of Internet service providers[60]—those who connect users to the Internet, such as cable companies, telephone companies, and wireless service providers.[61] The first filtering method—hardware content filtering—is highly controversial; the second method—service provider content filtering—is applied not only by oppressive regimes but also by democratic countries,[62] and certainly has merit when used to enforce decisions by courts or administrative agencies.[63] However, unless it is based on a

enforcement actions, or they do not want to lose existing markets as a result of their own non-compliance, or they want to preserve their option to enter into prospective markets in the future. Additionally, many smaller businesses do not have the resources to relocate their operations to avoid regulation; therefore, no exodus to minimum-regulation jurisdictions occurred. Instead, many actors on the Internet strive to comply with local regulation and employ geolocation tools to achieve that goal.

[59] Not all enforcement of laws on the Internet relies on the territorial partitioning of the Internet. *See, e.g.*, Stop Online Piracy Act, H.R. 3261, 112th Cong. § 102(c)(2)(C) (2011) (proposing to bar online payment providers from doing business with websites that breach the law). Such proposals raise a number of issues, including their potential extraterritorial effects.

[60] *See infra* notes 320–22 and accompanying text (on filtering by service providers); *see also* FREEDOM ON THE NET: A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA 6–7 (Sanja Kelly & Sarah Cook eds., Freedom House, 2011).

[61] The term "Internet service provider" as used here does not match the statutorily defined term "service provider." *See* 17 U.S.C. § 512(k)(1) (2010) (defining "service provider" to cover a wider range of entities).

[62] *See* Jonathan Zittrain & Benjamin Edelman, *Documentation of Internet Filtering Worldwide*, BERKMAN CTR. FOR INTERNET & SOC'Y-HARV. L. SCH., http://cyber.law.harvard.edu/filtering/ (last updated Oct. 24, 2003).

[63] For instance, a court may order Internet service providers to block access to a website that does not comply with a court's decision according to local regulations against pornography. It is more problematic if a government requests that service providers filter for pornography and block the content without any formal proceedings to establish the illegality of the particular content. *See also* Twentieth Century Fox Film Corp. v. British Telecomms. PLC, [2011] EWHC (Ch) 2714 (Eng.) (for a decision in the context of copyright infringement); Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, art. 25(2), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF.

decision concerning particular individual content, no type of content filtering appears to be an acceptable means for achieving routine compliance with local laws and regulations; usually, these methods of filtering are viewed by the public with significant skepticism, if not outrage. Academics have argued that the two types of filtering should be prohibited as being contrary to the freedom of speech,[64] and recently the Court of Justice of the European Union ruled that court-imposed, time-unlimited, general filtering violates the European Union Charter of Fundamental Rights and other EU legislation.[65]

The third method of raising borders on the Internet leaves the burden upon responsible website operators[66] and requires that they take actions necessary to comply with territorially-defined obligations. This method has several advantages. First, it avoids the public outrage associated with governmental intrusions into Internet traffic[67] and potential constitutional and human rights challenges that can arise because the intrusions may have the character of censorship of speech.[68] Second, the method relies on

---

64 *See infra* notes 319–22 and accompanying text; *infra* Part IV.B.3.

65 *See* Case C-70/10, Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=763036. The CJEU noted that the filtering at issue would violate the rights of not only Internet users—"their right to protection of their personal data and their freedom to receive or impart information,"—but also Internet service providers—"the freedom to conduct business." *Id.* at ¶¶ 49, 50. The filtering was also held to be in breach of the EU E-Commerce Directive (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market) and other related EU directives. *Id.* at ¶ 54; *see* case C-360/10, Belgische Vereinigung van Auteurs, Componisten en Uitgevers (SABAM) v. Netlog NV (2012); *see also infra* note 67.

66 *See supra* note 6 (defining the term "website operator" as used in this article).

67 *See, e.g.*, Björn Greif, *Löschen Statt Sperren: Bundesregierung Kippt Zugangserschwerungsgesetz*, ZDNET (Apr. 6, 2011), http://www.zdnet.de/news/digitale_wirtschaft_internet_ebusiness_loeschen_statt_sperren_bundesregierung_kippt_zugangserschwerungsgesetz_story-39002364-41551361-1.htm (describing the recent developments surrounding Zugangserschwerungsgesetz in Germany and the Digital Economy Act in the United Kingdom); Josh Halliday, *Digital Economy Act: Filesharing Code Delayed by Six Months*, THE GUARDIAN (Apr. 5, 2011), http://guardian.co.uk/technology/2011/apr/05/digital-economy-act-filesharing.

68 *See infra* Part IV.B.3 (discussing the constitutional aspect of the problem).

the parties who actually know the content of the website at any given moment and who should be able to assess their legal obligations in various territorial contexts.[69] Third, the method does not challenge the status of Internet service providers as common carriers eligible for safe harbors that protect them from secondary liability.[70] The safe harbors are based on the theory that common carriers are unaware of the content that they carry and are technically incapable of efficient monitoring of the content that would allow them to prevent direct infringements. If governments require and service providers execute the filtering of certain content, the common carrier status could be in jeopardy.

The third method of raising borders on the Internet through website operators is arguably preferable to the second method that relies on filtering by Internet service providers; website operators are better positioned to limit access to their websites to users from certain countries or block access to users from other countries. Website operators have utilized geolocation tools to achieve this goal.

---

[69] The situation is more complicated when operators, such as eBay or YouTube, provide space for users to post their own content; the degree to which such operators are able to monitor the content uploaded by the users is subject to debate. *E.g.*, *Content ID*, YOUTUBE, http://www.youtube.com/t/contentid (last visited Nov. 19, 2011). For a choice-of-law perspective on the problem of potential operator liability for the conduct of users, see generally Graeme B. Dinwoodie et al., *The Law Applicable to Secondary Liability in Intellectual Property Cases*, 42 N.Y.U. J. INT'L L. & POL. 201 (2009). *See also* Case C-70/10 Scarlet Extended SA v. Société Belge des Auteurs Compositeurs et Éditeurs (2011), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=64604.

[70] Internet service providers, or website operators operating search engines or public fora for users' content, would not be the responsible parties if their liability is limited by a safe harbor provision. *See, e.g.*, Digital Millennium Copyright Act, 17 U.S.C. § 512(g)(2) (2010); Communications Decency Act, 47 U.S.C. § 230(c) (2006); Directive 2001/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, arts. 12–15, 2000 O.J. (L 178) 1, 3.

## II. GEOLOCATION TOOLS

Before the next Part discusses cybertravel as the evasion of geolocation, this Part reviews what geolocation tools are, who uses them and for what purposes, and how the tools operate. As explained earlier, geolocation tools have become one of the means of erecting borders on the Internet; the tools can determine where an Internet user is physically located and allow tailored content to be delivered to that user based on the local regulatory framework and other localized preferences. Currently these tools utilize Internet protocol ("IP") addresses[71] to localize Internet users; however, in the future, geolocation tools might not need to rely on IP addresses at all or solely on IP addresses[72]—additional or different data points may serve as sources of information about an Internet user's location.

### *A. Use of Geolocation Tools*

If we regard the territorial partitioning of the Internet as an undesirable outcome (meaning detrimental to the original idea of the network),[73] the story behind geolocation tools might indeed be another example of Tim Wu's vicious "Cycle"[74] because these tools—like other technologies subject to Wu's "Cycle"—had innocent beginnings. Apparently, the first desire to find out where Internet users were located arose in the advertising industry when advertisers wanted to target advertisements based on a user's location.[75] So, if you opened a page on your home computer, the advertisers wanted you to be offered meals at your local restaurants; if you opened the same page on your laptop while connected to the Internet at a Chicago airport, the advertisers wanted you to see advertisements for local Chicago restaurants.

---

71 *See infra* Part II.B (explaining the term "IP address").

72 *See infra* notes 163–64 and accompanying text.

73 "The bordered Internet is widely viewed to be a dreadful development that is antithetical to the Internet's 'true' purposes and undermines the Internet's promise." GOLDSMITH & WU, *supra* note 26, at 150.

74 *See* Wu, *supra* note 53; *supra* Part I.

75 "To the best of my knowledge, commercial Internet-based geographic analysis tools have been available since no later than 1999 . . . ." Edelman, *supra* note 9, at 2. On the history of geolocation see GOLDSMITH & WU, *supra* note 26, at 58–61.

Although it might be annoying to some that connecting to the Internet during a short layover at the Frankfurt airport results in Google assuming that you wish to use the German version of their search engine,[76] the general Internet population appears to prefer the convenience of localized content.[77]

After they were applied in advertising, geolocation tools began to be employed by those who were attempting to comply with territorially-defined regulation. Regulation continues to be territorial; even in highly internationally-harmonized areas such as copyright, differences among the laws of countries persist, so it is desirable to tailor the accessibility of content on the Internet to the requirements and limitations of individual countries. Website operators use geolocation tools to comply with various regulatory requirements—for instance, to satisfy restrictions that the U.S. government imposes on exports to certain countries.[78] Companies may use geolocation tools to prevent customers from certain countries from ordering electronic equipment because of safety requirements that the particular country imposes on such equipment sold for use in that country. Even if parties regulate their affairs between themselves by private contract—for instance,

[76] Although the German version of the website appears automatically, you can manually switch it back to Google.com.

[77] "[T]he explosive growth of the World Wide Web is directly attributable to the invention of identification and filtering technologies that made it possible to organize and select from the morass of available information." Goldsmith, *supra* note 35, at 1228–29. "[G]eographical borders first emerged on the Internet not as a result of fiats by national governments, but rather organically, from below, because Internet users around the globe demanded different Internet experiences that corresponded to geography." GOLDSMITH & WU, *supra* note 26, at 49. On the various virtues of localized content, see *id*. at 50–53. Some website operators believe that users want websites to go even further and offer not only localized but also individualized content. Thus, if you like Indian food, when connecting to the Internet from Chicago, not only will you see only ads for Chicago restaurants, but those ads will be limited to restaurants serving Indian food. While localization of content may always be achieved by applying geolocation tools without retaining identifiable data on user behavior, individualization of content requires the collection and retention of identifiable data on individual users, which creates personal data protection issues. *See infra* Part IV.B.1 (discussing anonymization).

[78] Michael Geist mentioned that Microsoft was using geolocation tools "to comply with U.S. regulations prohibiting the export of strong-encryption Web browser software." Geist, *supra* note 41, at 334.

by obtaining a copyright license for certain content—their contracts may be limited territorially.

Often the uses of geolocation serve multiple purposes.[79] For example, online gaming websites use geolocation tools both to comply with local gaming regulations and to prevent fraud.[80] First, geolocation is employed to help ensure that customers will not access gaming sites from countries that impose prohibitions or limitations on Internet gaming.[81] William Hill, one of the largest bookmakers in the United Kingdom and also an online gaming operator, uses geolocation tools to prevent U.S. players from accessing its gaming products that are legal in the United Kingdom, but expose various entities involved in the operation to liability in the United States.[82] The second purpose for which the gaming industry uses geolocation tools is to identify potential credit card fraud.[83] If the address given to the issuing bank does

[79] TV stations and other online content providers may have various reasons for limiting access to content from certain countries—copyright licensing issues are not the only reason. *See infra* note 180; *see also Frequently Asked Questions: BBC Help*, BBC http://faq.external.bbc.co.uk/questions/ bbc_online/website_changes (last visited July 28, 2011). As a result of these various limitations, for instance, you cannot access episodes of *The Tonight Show* when you are in Germany; the NBC website will not play the video once it detects your foreign location. THE TONIGHT SHOW, http://www.nbc.com/the-tonight-show/ (last visited Nov. 19, 2011). Similarly, the German television station SAT1 will not allow you to watch *Kommissar Rex* from a U.S. location; upon opening the webpage you will receive a message explaining that the content is not available in the United States. KOMMISSAR REX, http://www.sat1.de/filme_serien/rex/ (last visited Nov. 19, 2011). Users have reported that Netflix will not allow them to download a film if they access their U.S. Netflix account from a location outside the United States. I am indebted to my colleague, Professor Stacey Tovino of the William S. Boyd School of Law, for the observation about Netflix. Other Netflix users have reported the same problem.

[80] *See generally* JULIA HÖRNLE & BRIGITTE ZAMMIT, CROSS-BORDER ONLINE GAMBLING LAW AND POLICY (2010); *see also* Tricia Lines Hill, *Harnessing the Power to Stop Fraud*, IVERTECH, http://software.ivertech.com/_ivertechArticle15229_ HarnessingthePowerto StopFraud.htm (last visited Nov. 19, 2011).

[81] I am indebted to Gregory R. Gemignani of Lionel Sawyer & Collins, Las Vegas, Nevada, for an insightful discussion about the uses of geolocation in the gaming industry.

[82] WILLIAM HILL, http://casino.williamhill.com/ (last visited Nov. 19, 2011).

[83] On geolocation in preventing credit card fraud see GOLDSMITH & WU, *supra* note 26, at 61; *see also* Hill, *supra* note 80; Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61, 76 (2011).

not match the physical address that is self-reported by the Internet user at registration (as confirmed by the geolocation tools), the operator is alerted and may take additional measures to ensure that the player is a legitimate user of the credit card.

The list of reasons for the voluntary use of geolocation tools goes beyond achieving legal compliance or preventing fraud, and includes purposes such as implementing differential pricing, localizing advertising, and Internet searching. Of course, illegal operations also utilize the tools in support of their illegal activities.[84] A Hong Kong website operator, who purposefully engaged in activities that appeared to infringe intellectual property rights, used the tools to limit the site's exposure to local authorities by making sure that it did not infringe any rights in Hong Kong. To meet this goal, the company employed geolocation tools to make sure that no user from Hong Kong could download an infringing work posted on its website, but simultaneously permitted users connected from other countries to download the content.[85]

In an important development for the future of geolocation, and consequently also for the future of cybertravel, governments are turning to geolocation as an enforcement tool—a means to force Internet actors to comply with regulatory decisions and court orders. For example, regulators in Italy have mandated that gaming websites use geolocation tools to prevent users located in Italy from accessing certain content.[86] The U.S. Department of

[84] For this example I am indebted to Douglas Clark of Hogan Lovells International LLP, Shanghai, China.

[85] *See* MEGAUPLOAD, http://www.megaupload.com/ (last visited Nov. 19, 2011). For information on cross-border enforcement difficulties in intellectual property cases see generally Marketa Trimble, *Cross-Border Injunctions in U.S. Patent Cases and Their Enforcement Abroad*, 13 MARQ. INTELL. PROP. L. REV. 331 (2009) [hereinafter Trimble, *Cross-Border Injunctions*]; Marketa Trimble Landova, *The Public Policy Exception to Recognition and Enforcement of Judgments in Cases of Copyright Infringement*, 40 INTL. REV. INTELL. PROP. & COMPETITION L. 642 (2009).

[86] According to NeuStar (formerly Quova), a geolocation tools provider, "[g]eolocation technology is a requirement in online licensing applications in Italy. . . . An operator wishing to obtain an online gaming licence in Italy is required to note during its license application the technology that will be used for geolocation. . . . The use of geolocation technology is required in order to enable an operator to identify the

Justice made it a condition of its agreement with PokerStars, an online gaming company operating from the Isle of Man,[87] that the company "utilize geographic blocking technology relating to I.P. addresses."[88] In Germany, several courts have unequivocally accepted geolocation as "a viable and technically feasible method of determining website visitors' location[s]"[89] and ordered online gaming operators to utilize geolocation tools to limit access to certain content from particular German states.[90] Recent legislative efforts also show the need for clear jurisdictional borders on the Internet, whether they are efforts in the areas of Internet commerce[91] or online gaming.[92]

geographical origin of the player who attempts to access the gaming website. This is needed in order to prevent Italians having access to non-authorised sites managed by the same operator. . . . France has studied Italy's model and has developed a similar system which is expected to come into force some time during the year." NEUSTAR, *Geolocation; Ensuring Compliance with Online Gaming Regulations* 6 (2010), www.neustar.biz.

87 *About PokerStars*, POKERSTARS.NET, http://www.pokerstars.net/about/ (last visited Nov. 19, 2011).

88 Letter from Preet Bharara, U.S. Att'y, S.D.N.Y., to David M. Zornow, et al., Partners, Skadden, Arps, Slate, Meagher & Flom LLP (Apr. 19, 2011), *available at* http://www.rakeback.com/images/doj-pokerstars-domain-name-reinstatement.pdf. In this case, the U.S. government's leverage over the company has been the company's U.S.-registered domain name.

89 *See* Oberverwaltungsgericht Nordrhein-Westfalen [OVG] [Higher Administrative Court] July 2, 2010, BECK-ONLINE DATENBANK [BECKRS] 50510 (Ger.) (the decision refers to other German cases in which the German courts agreed that geolocation may be used to comply with their territorially-limited decisions); Oberverwaltungsgericht Nordrhein-Westfalen [OVG] [Higher Administrative Court] July 13, 2010, BECK-ONLINE DATENBANK [BECKRS] 51049 (Ger.). On the initial approaches by German courts to the use of geolocation see Michael Winkelmüller & Hans-Wolfram Kessler, *Territorialisierung von Internet-Angeboten – Technische Möglichkeiten, völker-, wirtschaftsverwaltungs- und ordnungsrechtliche Aspekte*, 5 GEWARCH 181, 181–83 (2009).

90 *But cf.* Oberverwaltungsgericht Lüneburg [OVG] [Higher Administrative Court] Apr. 3, 2009, BECK-ONLINE DATENBANK [BECKRS] 33166 (Ger.) (an earlier opinion by a German court concerning geolocation). "[I]t is not without a question whether at this time enough technically matured possibilities exist to exclude the Internet access only from Lower Saxony." *Id.*

91 *See, e.g.*, H.R. 10-1193, 67th Gen. Assemb., 2nd Reg. Sess. (Co. 2010) (enforcing online sales tax), enforcement temporarily stayed by an injunction.

92 *See, e.g.*, Unlawful Internet Gambling Enforcement Act of 2006, Pub. L. No. 109-347, §5362 (10)(B)(ii)(I), 120 Stat. 1952, 1955; H.R. 2267, 111th Cong., §5381(5)(B), §5383(b) (2009).

Sufficiently reliable geolocation tools,[93] if used appropriately and with due regard to protection of privacy,[94] could indeed assist in effective regulation and enforcement on the Internet.[95] Defined borders on the Internet would also benefit Internet actors who could deal with their rights on a country-by-country basis. Such partitioning makes entries into markets less costly for smaller entities because they do not have to bear the expense of a worldwide license, and country-by-country rights give right-holders the opportunity to maximize their profits by seeking the best licensing opportunities.[96]

---

[93] On accuracy of the tools see *infra* section II.B.

[94] For a project concerned with the protection of privacy (personal data protection) in geolocation see Barnes et al., *supra* note 8, at 5–6.

[95] Clarification of online jurisdictional boundaries for purposes of determining personal jurisdiction over an actor on the Internet would also be beneficial. Although courts in the world are refining their approaches to asserting personal jurisdiction over actors acting on the Internet, the tests leave Internet users with no clear rules. Some of the "low-tech" factors used in personal jurisdiction analyses appear to be losing relevance; for instance, the fact that a website utilizes a particular top-level country domain (such as .de or .fr) might not say much about the website's intentions to target or avoid users in a particular country when users no longer type in website addresses but instead locate websites through search engines that link users directly to the sites. With English becoming the universal language of the Internet it might be increasingly difficult to claim that a website in English is not directed at a jurisdiction in which English is not the primary or official language. *See* Joined Cases C-585/08 & C-144/09, Peter Pammer v. Reederei Karl Schluter GmbH & Co. KG *and* Hotel Aplenhof GesmbH v. Oliver Heller, ¶ 84 (2010), *available at* http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri =CELEX:62008CJ0585:EN:HTML (noting that "the language or the currency used . . . do not constitute relevant factors for the purpose of determining" personal jurisdiction). Similarly, the fact that a website is interactive, although originally viewed by courts as a determinative factor in the personal jurisdiction inquiry, is no longer considered determinative on its own by many courts. *See, e.g.*, *id.* at ¶ 79 (noting that the distinction between "interactive" and other websites "is not decisive"); *see also* Illinois v. Hemi Grp. LLC, 622 F.3d 754, 758 (7th Cir. 2010). The fact that a website employs geolocation tools might be a persuasive argument for the absence of personal jurisdiction over a website operator who uses the tools to prevent users from certain jurisdictions from accessing its website. *See generally* King, *supra* note 83 (discussing geolocation tools and personal jurisdiction).

[96] It is possible that the right owner may determine that a worldwide license is the best option; however, partitioning may give the right owner a bargaining advantage. For a contrary view in the context of the EU single market see Joined Cases C-403/08 & C-429/08, Football Ass'n Premier League Ltd. et al. v. QC Leisure et al. *and* Karen Murphy v. Media Prot. Svcs. Ltd. (2011), *available at* http://eur-lex.europa.eu/Lex UriServ/LexUriServ.do?uri=CELEX:62008C0403:EN:HTML.

### *B. Operation of Geolocation Tools*

Geolocation in the broadest sense is any means of detecting an Internet user's location. The raison d'être of geolocation tools is the determination of the physical location of a user; the tools are not designed to identify or track a particular user. Although they may use information that identifies a particular device that is used to access the Internet, such information is not necessarily sufficient to identify a particular user.[97] Absent implantation of a device into a human body, it will remain a challenge to attribute acts on the Internet to a particular human actor if more than one person has access to a device.[98] Despite this shortcoming, geolocation tools are being designed, used, and constantly improved because of the value that is attached to the ability to identify a user's location.

The most basic geolocation tools are based on self-reporting. For instance, an Internet website that requires registration asks a user for his location. Based on the information input by the user, the website tailors the content according to the regulations of the country where the user is located.[99] Another self-reporting mechanism offers users a list of countries in a dropdown menu, and after the user selects a country, the website directs the user to

---

[97] In cases of dynamically assigned IP addresses, the same IP address may lead to different devices at different times. Statically assigned or embedded IP addresses can identify a particular device but cannot link the device to a particular user if several users have physical or virtual access to the device. For more on statically and dynamically assigned IP addresses see *infra* notes 107–15 and accompanying text. A device may also be identified by "fingerprinting" methods that can recognize the same machine repeatedly by various indicators other than—or in combination with—an IP address. *See, e.g.*, PANOPTICLICK, http://panopticlick.eff.org/ (last visited Nov. 19, 2011).

[98] Former Google CEO Eric Schmidt was quoted as commenting on the need for attribution on the Internet: "In a world of asynchronous threats, it is too dangerous for there not to be some way to identify you. We need a [verified] name service for people. Governments will demand it." Gareth Beavis, *Schmidt: We Can Predict Where You Are Going to Go*, TECHRADAR (Aug. 6, 2010), http://www.techradar.com/news/internet/schmidt-we-can-predict-where-you-are-going-to-go-708339.

[99] This is what Seth Finkelstein called "co-operative geo-location" as opposed to "oppositional geo-location." "[I]t is in the interests of the party being located to co-operate with supplying geographic information, in order to gain some benefit." Expert Report of Seth Finkelstein, Nitke v. Ashcroft, 253 F. Supp. 2d. 587 (S.D.N.Y. 2003) (No. 01 Civ. 11476).

its country-specific pages.[100] Self-reporting is certainly sufficient for advertising purposes or for purposes of facilitating convenient content (such as pricing in local currency), but it is certainly not a tool for enforcement. Even if the self-reporting is part of a user agreement or licensing agreement, the benefits of the agreement or the threat of contractual sanctions under the agreement may not be sufficient incentives for users to report accurate information. However, if the self-reported location data are reliable, and if they are collected and retained, they may be used to recognize the same user in the future[101] or help identify the location of additional users.[102] Naturally, any such activity raises serious privacy concerns.[103]

[100] *See, e.g.*, BRITISH AIRWAYS, http://www.britishairways.com/travel/country_choice/public/en_us (last visited Nov. 19, 2011).

[101] "A simple way to find out the geographic location of a user visiting a Web site is to ask them . . . Location data, once entered, can thereafter be associated with a client IP address." James A. Muir & Paul C. Van Oorschot, *Internet Geolocation: Evasion and Counterevasion*, ACM COMPUTING SURVEYS, Dec. 2009, at 4:1, 4:8.

[102] Three experts who work for Facebook have estimated the location of users based on their "friends" in social media, thus exploring the probability of friendship as a function of distance. Lars Backstrom et. al., *Find Me If You Can: Improving Geographical Prediction with Social and Spatial Proximity*, WORLD WIDE WEB CONFERENCE, 61 (Apr. 26–30, 2010), http://delivery.acm.org/10.1145/1780000/1772698/p61-backstrom.pdf?ip=150.108.239.43&acc=ACTIVE%20SERVICE&CFID=64593187&CFTOKEN=55291539&__acm__=1328312060_1287e167fe6e65e8e6f255474345c4ab (a paper presented at the 2010 World Wide Web Conference).

[103] "If IP addresses are considered 'personal data' or 'personal information' for privacy purposes, the collection, use and disclosure of such information may be seriously restricted." Dan Jerker B. Svantesson, *Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet*, 23 J. MARSHALL J. COMPUTER & INFO. L. 101, 134 (2004) [hereinafter Svantesson, *Placing Boarders*]. *See* Bundesgericht [BGer] [Federal Supreme Court] Sept. 8, 2010, 136 ENTSCHEIDUNGEN DES SCHWEIZERISCHEN BUNDESGERICHTS [BGE] II 508 (Switz.) (discussing IP addresses as personal data); Jennifer Valentino-Devries & Emily Steel, *"Cookies" Cause Bitter Backlash*, WALL ST. J. (Sept. 19, 2010), http://online.wsj.com/article/SB10001424052748704416904575502261335693370.html ("Since July, at least six suits have been filed in U.S. District Court for the Central District of California against websites and companies that create advertising technology, accusing them of installing online-tracking tools that are so surreptitious that they essentially hack into users' machines without their knowledge. All of the suits seek class-action status and accuse companies of violating the federal Computer Fraud and Abuse Act and other laws against deceptive practices."). *See* Barnes et al., *supra* note 8, at 5–6.

Other methods of identifying the location of Internet users involve reliance on information that is presumably difficult for users to conceal or change. For instance, any website that requires payment by credit card may use the purchaser's billing address as a reliable indicator of the user's location. An online store may conclude that most delivery addresses will coincide with a purchaser's location. An airline may assume that the country of departure on a plane ticket is an accurate proxy for the country where the traveler is located. These indicators are clearly not perfect; travelers do not always purchase tickets to depart from their current location, purchasers do not always buy from the same location to which they wish goods to be delivered, and people do not always carry credit cards with billing addresses that correspond to their current location. Although less susceptible to manipulation than self-reporting, these other methods also fail as sufficiently reliable enforcement tools.

Geolocation tools provide a higher, though also not perfect, degree of reliability. These tools rely on the IP addresses of devices with which users access the Internet and are known as "IP geolocation" tools.[104] IP addresses are often described as "analogous to . . . physical mailing address[es],"[105] because they allow for accurate transmittal and receipt of data.[106] As for their utility in localizing users, their use is more complicated than the use of physical addresses because often IP addresses are not static—meaning permanently assigned to particular devices—but are assigned dynamically (and temporarily)[107] to those devices. By

[104] "Informally, *Internet geolocation* is the problem of determining the physical location (to some level of granularity) of an Internet user. A related but more specific term is *IP geolocation*, which refers to the problem of locating an Internet host using only its IP address." Muir & Van Oorschot, *supra* note 101, at 2; *see also* SVANTESSON, http://www.svantesson.org/projects/geo-identification/free-geo-location-tools.aspx (last visited Nov. 19, 2011) (providing examples of free geolocation tools).

[105] Joshua J. McIntyre, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected As Personally Identifiable Information*, 60 DEPAUL L. REV. 895, 900 (2011).

[106] *See, e.g.*, McIntyre, *supra* note 105 (discussing IP addresses).

[107] Although it is possible to assign static IP addresses dynamically, this paper uses the term "dynamically assigned IP address" to refer to the practice of dynamically assigning an IP address for a temporary period of time.

analogy, imagine an apartment complex that has one street number and one hundred apartment numbers. A static IP address would be similar to a complete address with the street number and apartment number, which would never change and always identify the same apartment. Using a dynamically assigned IP address would be similar to using the address of the apartment complex main office, which assigns in rotation the reusable numbers 1 to 100 to the apartments as people rent various apartments in the building; in this case only the office would know at any given moment which apartment was identified as, say, apartment 57. Similarly, only Internet service providers know at any given moment which dynamically assigned IP addresses are assigned to which users.[108]

Dynamically assigned IP addresses have become a standard feature of Internet connections since IP addresses became scarce in recent years because of the exhaustion of all addresses that are available under the currently prevailing Internet protocol in use—IPv4.[109] Because of the insufficient supply of IP addresses under this protocol (and as of February 2011 all IPv4 addresses were officially assigned),[110] Internet service providers have commonly held a pool of reusable IP addresses that they assign to various users temporarily and reassign to other users as users log on and off the Internet. The successor to IPv4, IPv6,[111] offers 340 undecillion IP addresses[112] and therefore allows for static addresses to be assigned to or embedded in all individual Internet-connected

[108] Internet service providers know which IP address is assigned to which account; naturally, they cannot identify which particular user (person, family member, colleague) is actually accessing the Internet with the device using the IP address.

[109] Experts have warned about the shortage of available IP addresses, and "[a]s of 3 February 2011, the central pool of available IPv4 addresses managed by the Internet Assigned Numbers Authority (IANA) has been depleted." *IPv4 Depletion and IPv6 Deployment FAQs*, NO. RESOURCE ORG., http://www.nro.net/wp-content/uploads/2011/02/nro_depletion_deployment_faq.pdf (last visited Nov. 19. 2011).

[110] *See Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied*, ICANN (Feb. 3, 2011), http://www.icann.org/en/news/releases/release-03feb11-en.pdf.

[111] *See What is IPv6?*, IPV6 ACT NOW, http://www.ipv6actnow.org/ (last visited Nov. 19, 2011).

[112] *See id.* 340 undecillion is $3.4 \times 10^{38}$.

devices,[113] opening the way to new business models and technological innovations that may utilize advantages associated with certainty of identification and traceability of devices with permanent and identifiable IP addresses.[114] For now though, many IP addresses continue to be dynamically assigned.[115]

Once a device connects to the Internet it announces its IP address and thus allows others to geolocate it.[116] The problem with geolocation is that there is no centralized register of all IP addresses that lists corresponding physical devices;[117] lists exist

---

[113] *See* McIntyre, *supra* note 105, at 901 ("Unlike current IP addresses, IPv6 addresses will include a unique code dictated by a computer's hardware, in effect making IPv6 addresses globally unique and permanently assigned to particular devices. IPv6 is unlikely to suffer from the address exhaustion that plagues the current protocol: the new system creates a 128-bit address, providing for approximately 340 undecillion . . . possible addresses."). Naturally, this development worries those who are concerned about privacy on the Internet. *See, e.g.*, Shawn C. Helms, *Translating Privacy Values With Technology*, 7 B.U. J. SCI. & TECH. L. 288, 299 (2001) ("IPv6, a proposed TCP/IP protocol for Internet communication, could be the nail in the coffin of anonymity on the Internet.").

[114] For instance, household appliances may be connected to the Internet and easily recognized if they have static IP addresses. This raises important privacy issues. *See generally* Barnes et al., *supra* note 8.

[115] The adoption of IPv6 did not keep up with the growing needs for IP addresses, and since IPv4 addresses could be assigned dynamically the adoption of IPv6 was not an imperative. However, we will probably see an acceleration in the adoption of IPv6 now since IP addresses under IPv4 were finally exhausted in February 2011 and there is a dramatically growing number of devices that require connection to the Internet. *See* Dylan Tweney, *No Easy Fixes as Internet Runs out of Addresses*, WIRED (Feb. 3, 2001), http://www.wired.com/epicenter/2011/02/Internet-addresses/. Users may purposefully change dynamically assigned IP address by powering off and on their routers. *See* Riva Richmond, *Resisting the Online Tracking Programs*, N.Y. TIMES, Nov. 11, 2010, at B7, *available at* http://www.nytimes.com/2010/11/11/technology/personaltech/11basics.html.

[116] For an easy-to-understand explanation of the functioning of the traffic on the Internet, see Jonathan Zittrain, *Internet Points of Control*, *in* THE EMERGENT GLOBAL INFORMATION POLICY REGIME 203, 204–07 (Sandra Braman ed., 2004).

[117] This is what Dan Jerker B. Svantesson refers to as "source problems." *See* Dan Jerker B. Svantesson, *The Impact of Geo-location Technologies on Internet Content Licensing – Let the "Cat and Mouse" Game Begin*, Intellectual Property Forum, No. 63, Dec. 2005, at 25 [hereinafter Svantesson, *Cat and Mouse*]. On "circumvention problems" see *infra* note 130 and accompanying text; *see also* Edelman, *supra* note 9, at 3–4; Thomas Hoeren, *Zoning and Geolocation – Technische Ansätze zu einer Reterritorialisierung des Internet*, 1 MULTIMEDIA UND RECHT 3 (2007) ("[T]he decentralized management of the Internet means that there is no authoritative database of host locations.") [hereinafter Hoeren, *Zoning and Geolocation*]; Ethan Katz-Bassett et al.,

that provide some information but none are complete and updated in real time. Although geolocation tool providers use lists and databases—both publicly accessible lists and lists obtained from other sources[118]—these data sources are often not sufficient and the providers may complement the functioning of their tools by utilizing other geolocation techniques. In their 2009 paper *Internet Geolocation: Evasion and Counterevasion*, apparently the first scientific paper to address the technical issues of both geolocation and geolocation evasion comprehensively,[119] James A. Muir and Paul C. Van Oorschot provide an overview of other geolocation techniques.[120] Among the techniques they list are estimates based on the time that it takes for the device in question to respond to a ping request (a request for response) from another device with a known geographical location,[121] and estimates based on the routing of packets that carry information through the network.[122] Combinations of methods are reported to yield the best results.[123]

*Towards IP Geolocation Using Delay and Topology Measurements*, IMC'06, Oct. 25–27, 2006, *available at* http://dl.acm.org/citation.cfm?id=1177090.

[118] *See* Muir & Van Oorschot, *supra* note 101, at 4–8, 10; *see also* Bamba Gueye et al. *Constraint-Based Geolocation of Internet Hosts*, 14 IEEE/ACM TRANSACTIONS ON NETWORKING 1219, 1220 (Dec. 2006); *European Location Study*, PTOLEMUS CONSULTING GRP., 92 (July 2010), http://www.quova.com/downloads/wp-freestudylaunch0707.pdf (reporting that Quova used a list of locations of 2.6 billion IP addresses).

[119] There are earlier scientific papers on geolocation, but if they mention evasion at all, they do so only briefly. For legal papers on geolocation that mention evasion see *infra* note 133.

[120] *See generally* Muir & Van Oorschot, *supra* note 101.

[121] *See id.* at 8 ("However, the time for IP packets to travel between two hosts at fixed locations varies."); s*ee also* Katz-Bassett et al., *supra* note 117, at 72 ("[O]ur study reveals that techniques based solely on network measurements have inherent limitations."); *cf.* Gueye et al., *supra* note 118, at 1219 ("[W]e propose Constraint-Based Geolocation (CBG), which infers the geographic location of Internet hosts using multilateration with distance constraints, thus establishing a continuous space of answers instead of a discrete one. . . . Our experimental results show that CBG outperforms the previous geolocation techniques.").

[122] *See* Muir & Van Oorschot, *supra* note 101, at 10.

[123] On the effectiveness of combining several methods of geolocation see for example Backstrom et al., *supra* note 102, at 69 ("[T]he addition of social information to the task of predicting physical location produces measurable improvement in accuracy when compared to standard IP-based methods.").

The accuracy of geolocation tools is subject to debate;[124] less debate has occurred on the question of what degree of accuracy should be expected if these tools are to be considered tools of compliance with regulatory and enforcement measures.[125] Not surprisingly, entities that sell geolocation tools claim that their tools are highly effective;[126] critics tend to question the providers' data and point out that even if geolocation tool providers publish data on the effectiveness of their tools, it is difficult to verify the data because most providers "do not publish their results, nor detailed information about their methods."[127] Muir and Van Oorschot have also noted that the data reported by providers about the high accuracy of the tools "typically assume no evasive action by users."[128]

---

[124] For a discussion of opposing views on the issue of effectiveness of geolocation tools by two German Courts—the Bayerischer Verwaltungsgerichtshof and Thüringer Oberverwaltungsgericht—see for example Hörnle & Zammit, *supra* note 80, at 38–39. *See also* Verwaltungsgericht München [VG] [Administrative Trial Courts] Nov. 20, 2008, BECK-ONLINE DATENBANK [BECKRS] 40756 (Ger.); Verwaltungsgericht Karlsruhe [VG] [Administrative Trial Courts] Dec. 17, 2007, BECK-ONLINE DATENBANK [BECKRS] 33500 (Ger.).

[125] For an interesting discussion about the expected level of accuracy of geolocation for purposes of compliance with a court order, see Oberverwaltungsgericht Nordrhein-Westfalen [OVG] [Higher Administrative Court] July 2, 2010, BECK-ONLINE DATENBANK [BECKRS] 50510 (Ger.) ("[T]he appellant is not required to exclude perfectly participation from Nordrhein-Westfalen in its Internet game of chance. It is only ordered that measures [of geolocation as ordered by the court] be introduced by the deadline [set by the court] and thereby the access from Nordrhein-Westfalen is significantly limited."). *See generally* Trimble, *Cross-Border Injunctions*, *supra* note 85, at 349.

[126] *See Geolocation: Ensuring Compliance with Online Gaming Regulations*, *supra* note 86, at 8 ("Using IP Intelligence data from Neustar, Ladbrokes was able to comply with [a Dutch Supreme Court] ruling by blocking online users from locations inside the Netherlands–a task that was achieved with virtually 100% accuracy."); *see also European Location Study*, *supra* note 118. On the accuracy of geolocation tools, see also Svantesson, *supra* note 103, at 111 ff. For older data on other services, see Thomas Hoeren, *Geolokalisation und Glücksspielrecht (Teil 2)*, 5 ZEITSCHFRIFT FÜR WETT-UND GLÜCKSSPIELRECHT 311, 312–13 (2008) [hereinafter Hoeren, *Geolokalisation*]; Svantesson, *The Accuracy of Geo-Location*, *supra* note 28, at 13–15.

[127] *See* Edelman, *supra* note 9, at 6; Svantesson, *Placing Boarders*, *supra* note 103, at 112.

[128] Muir & Van Oorschot, *supra* note 101, at 21. On the question of the accuracy of geolocation tools see Svantesson, *The Accuracy of Geo-Location*, *supra* note 28, at 13–20.

It is questionable whether we should require impermeable barriers from website operators who utilize geolocation to comply with regulation,[129] and whether operators should be expected to detect geolocation evasion. Evasion techniques will continue to be developed and it might be technologically impossible to preempt their development and use. Perhaps this is where "code" in the legal sense cannot be unequivocally shaped by "code" in the technical sense; maybe this is one of the cases in which legal rules have to intervene and provide support for the technical solutions, which in this case are endangered by evasion techniques that enable cybertravel.

## III. EVASION OF GEOLOCATION

The seminal problem of geolocation is that techniques exist that allow users to thwart geolocation tools.[130] Ben Laurie, the expert who provided testimony on geolocation in the well-known *Yahoo!* case in France,[131] pointed out that, in fact, "it is *fantastically easy* to deliberately evade geolocation."[132] Notwithstanding the interest of governments and various actors on the Internet in geolocation as a means of achieving compliance with regulation and enforcement, and the fact that evasion may render geolocation largely ineffective, evasion techniques have been mentioned in the literature only marginally.[133] Even in the

[129] For "A Brief History of Geolocation and the Law" see Kevin F. King, *Geolocation and Federalism on the Internet: Cutting Internet Gambling's Gordian Knot*, 11 COLUM. SCI. & TECH. L. REV. 41, 59–63 (2010); *see also* Trimble, *Cross-Border Injunctions*, *supra* note 85, at 349.

[130] *See* Svantesson, *Cat and Mouse*, *supra* note 117, at 25 (referring to these techniques as "circumvention problems."); *see also* Hoeren, *Zoning and Geolocation*, *supra* note 117.

[131] For the response in the United States to the litigation in France, see Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 433 F.3d 1199 (9th Cir. 2006). Ben Laurie was also a founding director of the Apache Software Foundation. *See Ben Laurie*, WIKIPEDIA, http://en.wikipedia.org/wiki/Ben_Laurie (last visited Dec. 19, 2011).

[132] *See* Declaration of Bennet Laurie in Lieu of Direct Testimony at 12, Nitke v. Ashcroft, 253 F. Supp. 2d 587 (S.D.N.Y. 2005) (No. 01 Civ. 11476) (emphasis added).

[133] *See, e.g.*, Svantesson, *Cat and Mouse*, *supra* note 117, at 24–30; Hoeren, *Zoning and Geolocation*, *supra* note 117; Thomas Hoeren, *Das Pferd frisst keinen Gurkensalat* –

scientific literature it was not until December 2009 that the first paper was published that focused fully on the techniques for evading geolocation.[134] Although a number of legal papers have been authored on geolocation and its legal implications, only two short articles[135] have addressed the legal issues associated with geolocation evasion tools or cybertravel.[136] However, interest in cybertravel will increase as geolocation becomes omnipresent and evasion tools even more user-friendly than they are today.

A spectrum of evasion techniques is available and a variety of providers offer means of evasion with various levels of sophistication.[137] Of course, remote access to computers that would have resulted in evasion of geolocation existed long before some of the current "mainstream" cybertravel tools emerged. For example, the Telnet and SSH protocols both allow logins to remote computers, and today commercial services such as GoToMyPC[138] and LogMeIn[139] make it easy for a user to remotely access a computer located anywhere in the world, thereby facilitating the

*Überlegung zur Internet Governance*, 36 NEUE JURISTISCHE WOCHEN 2615 (2008); Hoeren, *Geolokalisation*, *supra* note 126; King, *supra* note 83, at 71.

134 Muir & Van Oorschot, *supra* note 101, at 2 ("In contrast to our work, the academic literature to date on Internet geolocation techniques . . . has generally implicitly assumed that no evasive action is being taken."). *Id.* at 21 ("[W]e know of no open study of evasive geolocation prior to the present article, a preliminary version of which was captured in a technical report [in 2006]."). The technical report is available at http://www.scs.carleton.ca/research/tech_reports/2006/download/TR-06-05.pdf (last visited Nov. 19, 2011). For an earlier paper discussing evasion techniques see Edelman, *supra* note 9.

135 *See* Svantesson, *Cat and Mouse*, *supra* note 117, at 24–30; Sven Mitsdörffer & Ulf Gutfleisch, *"Geo-Sperren" – wenn Videoportale ausländische Nutzer aussperren: Eine urheberrechtliche Betrachtung*, 11 MULTIMEDIA UND RECHT 731 (2009).

136 Other than in the articles noted *supra* in footnote 135, the possibility of evasion is mentioned only as a side note in the literature. *See, e.g.*, Johnson & Post, *supra* note 49, at 1374 (brief mention of the possibility to "simply reconfigure [the user's] connection so as to appear to reside in a location outside the particular territory.").

137 This Part leaves aside instances of "accidental cybertravel"—instances in which an Internet user's IP address is altered without the user's knowledge or intent. *See* Backstrom, et al., *supra* note 102, at 61; Expert Report of Ben Laurie at 17, Nitke v. Ashcroft, 253 F. Supp. 2d 587 (S.D.N.Y. 2005) (No. 01 Civ. 11476).

138 *See* GOTOMYPC, http://www.gotomypc.com/remote_access/remote_access (last visited Nov. 19, 2011).

139 *See* LOGMEIN, https://secure.logmein.com/ (last visited Nov. 19, 2011).

use of the remote computer's Internet connection and foreign IP address. This type of cybertravel can be described as "self-sustained" because it is facilitated by equipment that a user may own or have available through family or friends in another country.[140] As opposed to these "self-sustained" cybertravel methods, the "mainstream" cybertravel tools that are described below do not rely on a user's own equipment or equipment to which a user specifically secures access in advance.

Most Internet users who remember the beginnings of the Internet are familiar with the most basic geolocation evasion technique, although they do not usually think of it as a tool for evading geolocation. It is the use of a dial-up connection to an Internet service provider phone number in a foreign country.[141] Once connected to the foreign dial-up service provider, the user is assigned an IP address for that country by the foreign provider, and it appears as if the user is located in the foreign country. The problems with this technique are the cost and speed of the connection. The speed problem is familiar to anyone who has ever used a dial-up connection, and calling a telephone number in a foreign country for an extended period of time can still be expensive. Although subject to these disadvantages, this form of cybertravel could be the only cybertravel available if a government shuts down the Internet throughout the country by ordering all Internet service providers to stop providing access to the network, as the government of Egypt did in January 2011.[142]

---

[140] The use of a user's own equipment makes the "self-sustained" cybertravel similar to the Slingbox concept. *See infra* note 259.

[141] *See* Muir & Van Oorschot, *supra* note 101, at 13.

[142] *See* Evgeny Mozorov, *Egypt Action May Spread Internet Kill Switch Idea*, SAN FRANCISCO CHRONICLE (Feb. 6, 2011), http://www.sfgate.com/cgibin/article.cgi?f=%2Fc%2Fa%2F2011%2F02%2F05%2FINO91HHD7P.DTL. Although it was the situation in Egypt in January 2011 that raised general attention to the problem of governmental interference with access to the Internet, there were other instances of smaller countries (Nepal and Burma) engaging in the same tactics (in 2005 and 2007, respectively). *See* Christopher Beam, *Egypt Protest Internet Shut Off: How Did the Egyptian Government Turn Off the Internet?*, SLATE (Jan. 28, 2011), http://www.slate.com/id/2283000/. For a detailed account of the Internet disconnection in Egypt, see James Crowie, *Egypt Leaves the Internet*, RENESYS BLOG (Jan. 27, 2011), http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.

Another cybertravel technique involves the use of a proxy IP address: users connect to the Internet through special software or a website that reroutes their connection, shields their IP address, and uses its own, creating the appearance in cyberspace that the user is connected through another device in another location. The easiest of these proxy tools to use, but the least likely to function well enough to satisfy most purposes for which cybertravel is desired, is a website in which users insert the Internet addresses of pages blocked by geolocation tools. The website then opens the requested pages on the users' behalf.[143] The major problem with this system for users is that the requested websites easily recognize a proxy and can simply block all access by the proxy.[144]

Another type of proxy service is the easy–to–use subscription services that allow users, for a fee, to sign in on a website and be reconnected through a proxy. There are variations of these services based on the audience that they target; some services focus primarily on customers interested in anonymization—Internet users who are concerned about their privacy.[145] These services, such as *Anonymizer*,[146] promise anonymity on the Internet by rerouting users to a neutral IP address—an IP address that is located somewhere that "do[es] not create suspicion."[147] Some users wish to obtain an IP address from a particular country;[148] for instance, in addition to anonymization, *Anonymizer* also offers a

[143] *See, e.g.*, ANONYMOUSE, http://anonymouse.org/anonwww.html (last visited Nov. 19, 2011); MADMANWEB, http://www.madmanweb.com/anon.html (last visited Nov. 19, 2011).

[144] Svantesson has noted additional problems: because the websites are so easy to use they are quickly overloaded by users; additionally, they offer "only a limited number of countries one can appear to be located in." Svantesson, *The Accuracy of Geo-Location*, *supra* note 28, at 17–18.

[145] For more on anonymization and its relationship to cybertravel, see Part IV.B.2.

[146] *See* ANONYMIZER, http://www.anonymizer.com/ (last visited Nov. 19, 2011).

[147] *See How It Works*, ANONYMIZER, http://www.anonymizer.com/business/how_it_works.html (last visited Nov. 19, 2011).

[148] For instance, the following website offers advice on how to connect via a German IP address. Although the advice is of general application, the website targets users who wish to appear as if they are connected to the Internet from Germany. *See Change Your IP Address to Germany*, IPRIVACYTOOLS, http://www.iprivacytools.com/ip-address-germany/ (last visited Nov. 19, 2011).

Geographic Distribution technology, which allows users to select the geographical location of their proxy IP address.[149]

There are also services that specialize in cybertravel to certain countries. For instance, *My Expat Network*[150] provides connections to users who want to watch U.K. television programs but are located outside the United Kingdom and cannot access the programs because of geolocation. For £5 per month they can sign in to *My Expat Network* and watch all the television shows that are on U.K. websites as if they were connected from inside the United Kingdom.[151] The same provider offers the same service, for $6.50 per month, to users outside the United States who want to watch U.S. television programs but are unable to do so because they are connected to the Internet with an outside-of-the-U.S. IP address and face similar access restrictions.[152] Once they appear to be connected from inside the United States, these users may access not only television programs but any other content that may be viewed only from within the United States.

One free proxy service that is more sophisticated than the services described above utilizes a series of proxies, for instance "private proxies"—volunteers who provide access to their machines to people from other countries, such as political activists who fear detection and persecution in their own countries.[153] The *Tor* project,[154] which enjoys significant funding from the U.S. government,[155] uses a chain of proxies to protect its users,[156] who

---

[149] *See Success Stories*, ANONYMIZER, http://www.anonymizer.com/business/success_stories.html (last visited Nov. 19, 2011).

[150] *See* MY EXPAT NETWORK, http://www.my-expat-network.co.uk/ (last visited Nov. 19, 2011).

[151] *See id.*

[152] *See id.*

[153] *See Tor: Overview*, TOR, http://www.torproject.org/about/overview.html.en#thesolution (last visited Nov. 19, 2011).

[154] *See* TOR, http://www.torproject.org/ (last visited Nov. 19, 2011).

[155] About seventy-five percent of Tor funding comes from the U.S. government. Interview with Andrew Lewman, Executive Director, Tor, WBUR.ORG, Jan. 31, 2011, *available at* http://hereandnow.wbur.org/2011/01/31/egypt-Internet-government.

[156] *See* Karsten Loesing, et al., *A Case Study on Measuring Statistical Data in the Tor Anonymity Network, in* FC 2010 WORKSHOPS 203, 203–05 (R. Sion et al. eds., 2010); Muir & Van Oorschot, *supra* note 101, at 15; *Tor: Overview*, *supra* note 153.

are not only dissidents criticizing oppressive governments or persons avoiding government censorship,[157] but also journalists communicating with whistleblowers, and the U.S. Navy gathering intelligence.[158]

As are any evasive technical solutions, tools for the evasion of geolocation are also susceptible to detection, at least to some degree.[159] For instance, a Java applet in a webpage may lead to the identification of a user's true IP address,[160] and certain timing-based geolocation tools might be able to localize a user without the tools ever detecting the user's true IP address.[161] Providers of geolocation tools are constantly searching for ways to eliminate evasion and identify true IP addresses to determine the accurate geographic locations of Internet users. As one might expect, this is a constant race where it may take just a few weeks or months for the creators of evasion techniques to respond to improvements in geolocation tools and improve their techniques to further challenge geolocation.[162]

It is important to note that while cybertravel tools offered by various sources currently operate on the basis of IP addresses,

---

[157] *See* Loesing et al., *supra* note 156, at 203. "While the original goal of Tor was to enhance privacy, recently Tor has become popular amongst users who wish to circumvent national censorship systems, such as those in countries like Iran and China." *Id.* at 204. "[T]he statistics . . . indicate that Tor usage significantly increased from Iranian IP space in June 2009 after the Iranian elections." *Id.* at 206; *see also* Interview with Andrew Lewman, *supra* note 155.

[158] *See Tor: Overview*, *supra* note 153. For other ways to evade geolocation see Edelman, *supra* note 9; Muir & Van Oorschot, *supra* note 101, at 14.

[159] "Another problem is that Internet anonymizers (intermediate web servers that disguise the user's IP address) and remote Internet connections can, despite countermeasures by geo-ID firms, still sometimes defeat the identification process." GOLDSMITH & WU, *supra* note 26, at 62.

[160] *See* Muir & Van Oorschot, *supra* note 101, at 16; *see also* Hoeren, *Geolokalisation*, *supra* note 126.

[161] *See* Muir & Van Oorschot, *supra* note 101, at 18. Tools also exist to "fingerprint" a device; however, unless one of the identifying features contains location information, the fingerprinting does not localize the device.

[162] *Compare* Muir & Van Oorschot, *supra* note 101, at 3, *with* information by the founders of the Tor project at the Def Con 18 conference in 2010 in Las Vegas, Nevada. *See also Geographic Location/Privacy/geopriv*, IETF, http://datatracker.ietf.org/wg/geopriv/ (last visited Nov. 19, 2011).

cybertravel will not disappear simply because methods of locating Internet users other than methods based on IP addresses will be employed. Indeed, in the future other methods of tracking Internet users' geographical locations could replace the current geolocation tools that use IP addresses; either newly emerging or already existing means—for instance means based on the global positioning system ("GPS")—could become the norm for localizing Internet users.[163] Switching to any other means will not necessarily end cybertravel but will likely lead to the development of new evasion tools that will permit cybertravel under new conditions.[164]

## IV. THE LEGAL STATUS OF CYBERTRAVEL

It seems inevitable that the more geolocation is used to limit access to certain content on the Internet, the more users will cybertravel to bypass geolocation and access restricted content. Even in the absence of governmentally mandated use of geolocation by website operators, geolocation is likely to become widespread as website operators respond to the requirements of territorially-defined regulation on the Internet with a greater use of geolocation tools. The more emphasis that regulators place on territorial regulation, and the more that geolocation tools become the means of complying with that regulation, the more pressing it will become for there to be a legal conceptualization of cybertravel. This conceptualization will also be needed if in the future the need for attribution of acts on the Internet to particular devices leads to IP addresses or other location identifiers being embedded in Internet-connected devices; particularly in such an

[163] *See* Eric Goldman, *Geolocation and A Bordered Cyberspace*, TECH. & MKTG. L. BLOG (Nov. 13, 2007), http://blog.ericgoldman.org/archives/2007/11/geolocation _and. htm. On various methods of localizing devices see, for instance, Barnes et al., *supra* note 8, at 15–16.

[164] Even if IP addresses are embedded in devices—and even if they are permanently attached to particular persons (for instance, through implantation into the human body)—cybertravel will not necessarily be excluded, because tools are likely to continue to be developed that will allow users to bypass geolocation.

environment the desire for cybertravel will intensify.[165] It is therefore crucial and timely to determine whether cybertravel is a legal activity under present legal regimes and whether there are reasons for which cybertravel should be made or remain legal in the future. This Part discusses the current legal status of cybertravel and suggests how the law should treat cybertravel in the future—if there is or should be a future for legal cybertravel. It also reviews some technological and business solutions that may complement the future legal framework for cybertravel.

### *A. Is Cybertravel Legal?*

It is difficult to analyze all the legal aspects of cybertravel in the abstract because cybertravel is used for a wide variety of purposes, both legal and illegal, such as avoiding governmental regulation, bypassing limitations imposed because of the contractual obligations of website operators, or merely viewing advertisements created for a location other than the one in which the user sits.[166] However, it seems safe to state that there is one party involved in cybertravel that is unlikely to be exposed to liability: the website operator, who employs geolocation tools to make his website viewable only to users from certain countries, states, regions or locations.[167] In fact, if a website operator's decision to limit access to his website is based on a law-related purpose (rather than a business-related purpose), he will usually employ geolocation tools to restrict access to his website from certain countries precisely for the purpose of complying with his legal obligations rather than avoiding them.[168]

There are two parties that might be concerned about potential liability for their involvement in cybertravel and two acts in cybertravel that might lead directly or indirectly to liability.[169] The

---

[165] The same can be said for future devices that might be implanted into the human body, thereby allowing for identification of not only the device but also the particular person.

[166] *See supra* note 14 and accompanying text (commenting on the scope of this article).

[167] *See supra* Part II discussing geolocation tools.

[168] The Hong Kong Company mentioned in Part II.A would be one exception.

[169] Such liability may be both civil and criminal. *See infra* Part IV.A.

parties are the Internet user, who utilizes cybertravel tools to access restricted content, and the cybertravel tool provider, who facilitates cybertravel by offering and providing the cybertravel tools.[170] The two acts involved in cybertravel that may expose the user and the provider to liability are the act of viewing or using restricted content and the act of cybertravel itself as a method of circumventing tools used to restrict access to content. Although cybertravel providers might not view or use restricted content or cybertravel themselves, their facilitation of acts by users might subject the providers to liability.

This section discusses the various legal aspects of cybertravel. It reviews the potential for liability for both the cybertraveling user and the cybertravel provider while taking into account current law in both the United States and other countries, with particular emphasis on copyright law.

1. Liability of Cybertraveling Users

The initial problem in assessing potential cybertraveler liability is the problem of localization of their acts. Localization may determine not only the countries under whose laws a cybertraveler may be liable, but also often which countries' courts have personal jurisdiction over the cybertraveler. Regardless of whether a cybertraveler's other acts establish general jurisdiction in a country, cybertravel can generate specific jurisdiction over the user that emanates from the acts of cybertravel itself.

There are two approaches to the localization of the acts of cybertravel: the physical world approach and the cyberspace approach. The physical world approach is straightforward: anything that the user does is localized in the place of his physical location. Under this approach, when a user sits at his Internet-connected device in Chile and cybertravels to Germany by utilizing a German IP address, his acts are localized in Chile where he is physically located. If cybertravel enables the user to copy, without the copyright holder's authorization, content that is protected by copyright in Chile, the cybertraveler will be liable for

[170] *See supra* Part III discussing cybertravel tools.

copyright infringement in Chile—even if the content is made available on the website of a non-Chilean website operator and is stored on a server located outside of Chile. If Chile permits its courts to exercise personal jurisdiction based on tortious activity committed in their jurisdiction, Chilean courts will have personal jurisdiction over the user based on the user's acts in Chile.

The user in the example could also be liable for his actions in Germany if Germany had adopted the cyberspace approach to localization. The cyberspace approach follows the packets that carry information on the Internet and localizes acts based on the place or places in which the cybertraveler's physical acts (of typing on a keyboard) cause technological effects. For example, imagine that the user in Chile cybertravels to Germany to access copyrighted content on a website run by a German website operator that is protected by technological protection measures against viewing by users connected from outside Germany. If using cybertravel to bypass the measures and access the content without the copyright holder's authorization is illegal under German law,[171] liability for the act would arise in Germany because Germany is the place where the measures are breached (causing technological effects) to access the servers that store the content. Because Germany provides for the jurisdiction of German courts in the place of the effects of a tortious act, German courts have personal jurisdiction over the user in Chile based on the effects of the user's acts in Germany.[172]

Of course difficulties arise if, using the example above, the content on the website that permits access only to users connecting from Germany is stored on servers that are located in another country, such as the United States. In this scenario, the acts of

[171] *See infra* Part IV.A for a discussion of the European approach to liability for breaching technological protection measures.

[172] Council Regulation 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, art. 5(3), 2001 O.J. (L 12) 1; Case C-21/76, Handelskwekerij G. J.Bier B.V. v. Mines de Potasse d'Alsace S.A., 1976 E.C.R. 1735; Zivilprozessordnung [ZPO] Code of Civil Procedure, Sept. 12, 1950, Bundesgesetzblatt, Teil I (BGBl. I) 3202, as amended, § 32 (Ger.); ANDREAS RUFF, VERTRIEBSRECHT IM INTERNET 62 (2003).

breaching the protection measures and accessing the content without authorization would then technically occur in the United States. While liability might arise under U.S. law, establishing personal jurisdiction in the United States based on the acts may be difficult unless information about the location of the servers was available to the cybertraveler at the time of his acts and it can be claimed that he purposefully directed his actions at the particular forum where the servers were located. This is a general problem of personal jurisdiction on the Internet when purposeful direction of tortious acts is required and a user directs the acts at a specific forum, but the forum is unknown to him at the time of his acts.[173]

Even when users' acts occur while the users are cybertraveling to another country, the users may still be in breach of laws that prohibit them from viewing certain content or engaging in certain conduct in the country where they are physically located.[174] For instance, the online gambling laws of South Africa penalize not only companies that provide illegal online gambling in the jurisdiction of South Africa and Internet service providers who allow users in South Africa to access illegal online gambling websites, but the laws also hold liable users who gamble on such websites.[175] Therefore, if a user located in South Africa gambles

[173] For a discussion of the problem of acts on the Internet that are clearly directed at some forum but the identity of the forum is unknown to the user at the time of the act see Marketa Trimble, *Setting Foot on Enemy Ground: Cease-and-Desist Letters, DMCA Notifications and Personal Jurisdiction in Declaratory Judgment Actions*, 50 IDEA 777, 818–21 (2010) [hereinafter Trimble, *Enemy Ground*].

[174] This article provides a few examples of such laws but does not cover all the legal doctrines that may be invoked when a user cybertravels.

[175] In South Africa all three actors—the gambling website operator, the Internet service provider, and the end user—are liable for illegal online gambling. *See On-line Gambling Transactions Are Outlawed in South Africa*, GAUTENG GAMBLING BD., http://www.ggb.org.za/index.php?option=com_content&view=article&id=3:newsflash-2&catid=3:newsflash (last visited Nov. 19, 2011). Compare this with the situation in the United States, where the Unlawful Internet Gambling Enforcement Act of 2006 does not apply to players who place bets. Gerd Alexander, *The U.S. on Tilt: Why the Unlawful Internet Gambling Enforcement Act Is A Bad Bet*, 2008 DUKE L. & TECH. REV. 6, 29 (2008); *see also* Federal Wire Act, 18 U.S.C. § 1084 (2006); S. Rep. No. 588, 87th Cong., 1st Sess. (1961) (and its associated legislative history). *Cf.* also Strafgesetzbuch [StGB] [Penal Code], May 15, 1871, Reichsgesetzblatt [RGBl] 127, as amended, § 284–85 (on unlawful operating of gambling and participating in unlawful gambling).

on one of these websites, the user breaches South African law, and the fact that the user cybertravels to another country to do the gambling will probably not shield the user from liability under South African law nor from the personal jurisdiction of the South African courts.

What if the laws of the country of the user's physical location permit the user's acts but the acts are contrary to the laws of the country to which the user cybertravels? Will a user's cybertravel to a country where access to particular content or certain activities are prohibited lead to the user's liability in that country? While it may seem implausible that a user would purposefully cybertravel to a country to engage in an activity that is illegal under the laws of that country, such scenarios are possible. For example, a user might want to criticize the country's political leaders to an extent that would be deemed illegal in that country and wish to appear as though he were located in the country. In a particularly alarming scenario, a user may cybertravel to a country inadvertently—by being redirected randomly through an intermediate IP address in that country or by being assigned a final IP address in that country without the user's intent or knowledge.[176] While the physical approach to cybertravel would create no user liability in a country to which the user had cybertraveled, the cyberspace approach would result in user liability. However, the level of the interest of a country to which the user had cybertraveled in extending its prescriptive jurisdiction over a non-resident user or enforcing its laws against a non-resident user will vary according to the country's interest in regulating behavior by non-residents. For example, a country might have a minimal interest in enforcing its anti-online gambling laws against non-resident users, even if the country's courts could find grounds for extending their personal jurisdiction over non-resident users. A country might, however, have a much greater interest in extending its prescriptive and adjudicatory jurisdiction in a situation involving a restriction of speech[177] or attacks on computers located in the country.[178]

---

[176] *See supra* note 137 (discussing "accidental cybertravel").

[177] *See infra* notes 315 and 316.

a) Liability under Copyright Laws

Copyright law is a particularly pertinent area for review in the context of cybertravel because geolocation tools are often used as a means of compliance with copyright laws, which afford territorially-limited rights, and which, despite their significant level of international harmonization, still vary among countries.[179] Although a website operator, for example, may secure a license for particular content, the license may be restricted to one country or a limited number of countries. Website operators (or any licensee) may enter into licenses that are not worldwide for any number of reasons. First, the licensee might not have the necessary resources to pay for worldwide rights, and obtaining a license for a limited market could be the licensee's only option. Or, the licensor may decide not to license content in certain markets if the licensor plans to launch a country-specific version of the same content and does not want competition from foreign versions.[180] Further, the licensor may wish to implement a strategy for releasing the work in different countries in various media at various times. It is also possible that copyright in a particular work might not be held by the same right-holder in all countries and as a result there might be high transaction costs associated with locating all of the right-holders and negotiating licenses with all of them, and right-holders in some countries might simply not agree to a license. Because of the territorial limitations of licenses, website operators and other licensees use geolocation tools to limit access to licensed content

[178] *See infra* Part IV.A.1.b (discussing the applicability of anti-hacking laws to acts of cybertravel).

[179] Notwithstanding the great degree of international harmonization that has been achieved through several international treaties on copyright, copyright law is still a matter of national legislation and subject to national differences associated with certain flexibilities that are embedded in the treaties, occasional non-compliance with the treaties, and the fact that some issues of copyright law remain unaffected by international treaties.

[180] There are numerous examples of national versions of television shows that are made inaccessible to users from other countries where local national versions are available. *Dancing with the Stars* is an example. *See Outside the U.K.?*, BBC: STRICTLY COME DANCING, http://www.bbc.co.uk/strictlycomedancing/about/#outside_the_uk (last visited Apr. 12, 2012).

to users located only in the countries for which they have secured a license.[181]

A cybertraveler might be subject to liability if cybertravel is interpreted as an act of circumvention of geolocation, and if geolocation tools are considered tools that prevent access to or certain uses of a copyrighted work. Protection against the circumvention of tools that protect works from unauthorized acts was introduced at the international level by the 1996 WIPO Copyright Treaty[182] and the WIPO Performances and Phonograms Treaty[183] (the "WIPO Treaties"), which in Articles 11 and 18 respectively require countries that are parties to the Treaties to

> provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by [right-holders] in connection with the exercise of their rights . . . and that restrict acts . . . which are not authorized by the [right-holders] concerned or permitted by law.[184]

Provided that geolocation tools meet the required standard of effectiveness,[185] and cybertravel is viewed as a circumvention tool,

---

[181] It is important to note that without a partitioning of the Internet some licensees would not be in business if a worldwide license was required for content that they wanted to use on the Internet.

[182] World Intellectual Property Organization [WIPO] Copyright Treaty, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 65 (1997). The Treaty was signed by the United States in 1997, ratified by the United States in 1999, and entered into force for the United States in 2002. *Treaties and Contracting Parties*, WIPO, http://www.wipo.int/treaties/en/Remarks.jsp?cnty_id=1085C (last visited Feb. 8, 2012). The Treaty was implemented by the Digital Millennium Copyright Act, which was adopted in 1998. Digital Millenium Copyright Act, Pub. L. No. 105-304, 112 Stat. 28–60 (1998).

[183] World Intellectual Property Organization [WIPO] Performances and Phonograms Treaty art. 18, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 76 (1997).

[184] World Intellectual Property Organization [WIPO] Copyright Treaty art. 11, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 65 (1997); World Intellectual Property Organization [WIPO] Performances and Phonograms Treaty art. 18, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 76 (1997). For examples of technological protection measures see Stefan Bechtold, *Digital Rights Management in the United States and Europe*, 52 AM. J. COMP. L. 323, 325–31 (2004).

[185] It is unlikely that the fact that it is "*fantastically easy*" to evade geolocation tools, Laurie *supra* note 132, at 12, would impact their "effectiveness" for purposes of the anti-

the question becomes, at least under the language of the WIPO Treaties, whether the use of geolocation tools—the filtering of access based on a user's location—is used to restrict unauthorized or illegal acts.[186]

In line with the language of the WIPO Treaties, European laws that have implemented the WIPO Treaties and the corresponding

circumvention provisions. In the United States, technological protection measures have to be measures that, "in the ordinary course of [their] operation, require the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to work." 17 U.S.C. § 1201(a)(3)(B) (2006). In 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004), the court rejected the argument that a technological measure cannot be considered effective if its countermeasures are "widely available on the Internet." *Id.* at 1095. The court noted that the argument would be "equivalent to a claim that, since it is easy to find skeleton keys on the black market, a deadbolt is not an effective lock to a door." *Id.* See also Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000) (noting that the effectiveness of a technological measure does not depend on "whether or not it is a strong means of protection.").

In the United Kingdom Lord Justice Jacob commented on the term "effective technological measures" in a 2008 decision: "It is an odd phrase to use in English—in its context it clearly refers to something which is intended to have an effect rather than something which is invariably successful. If it meant the latter, then there would be no need to have a law preventing circumvention." Neil Stanley Higgs v. The Queen, [2008] EWCA (Crim) 1324, [27] (Eng.). In the United Kingdom a measure is considered "effective" if it "achieves the intended protection" by providing the copyright owner control of the use of the work "through . . . an access control or protection process . . . [or] a copy control mechanism." Copyright, Designs and Patents Act, 1988, c. 48, § 296ZF(2).

In Germany, geolocation tools that allow the restriction of access to users from certain countries would probably qualify under the definition of an *effective* technological measure as "an access control." Gesetz über Urheberrecht und verwandte Schutzrechte [UrhG] [German Copyright Act], Sept. 9, 1965, Bundesgesetzblatt, Teil I [BGBl. I] 3044, as amended, § 95a(2) (Ger.).

As the Oberlandesgericht München pointed out, the ineffectiveness of a technological protection measure cannot be concluded from the existence of a circumvention tool; "it is more determinative for the effectiveness of the protection measures whether they prevent an average user from infringing copyright." Oberlandesgericht München I [OLG I] [Higher Regional Court] Nov. 14, 2007, BECK-ONLINE DATENBANK [BECKRS] 23466 (Ger.). For a commentary on the issue of effectiveness from the EU perspective see Stefan Bechtold, *A Commentary on the 2001 EU Information Society Directive*, *in* CONCISE EUROPEAN COPYRIGHT LAW 343, 387–88 (Thomas Dreier, P. Bernt Hugenholtz eds., 2006).

[186] For a discussion of the problem from the Australian perspective see Svantesson, *Cat and Mouse*, *supra* note 117, at 27–28.

provision of the 2001 EU Information Society Directive[187] require that circumvention of technological measures be associated with a committed or potential unauthorized or illegal act.[188] For instance, a U.K. law provides protection for technological measures only to the extent that the measures aim at "prevent[ing] or restrict[ing] . . . acts that are not authorised by the copyright owner . . . and are restricted by copyright."[189] Since authorization is necessary only for acts that would infringe copyright if committed without authorization,[190] measures preventing a user from accessing a work for reasons other than to prevent acts of copyright infringement will not enjoy the protection that the law

[187] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, art. 6, 2001 O.J. (L 167) 10 [hereinafter 2001 EU Information Society Directive].

[188] Martin Senftleben, *a commentary on the 1996 WIPO Copyright Treaty*, *in* CONCISE EUROPEAN COPYRIGHT LAW 87, 111–12 (Thomas Dreier & Brent Hugenholtz eds., 2006).

> The requirement of a connection with the exercise of [the WIPO Copyright Treaty] or Berne rights reflects the principle expressed at the 1996 Diplomatic Conference that the protection of technological measures should complement the grant of exclusive rights so as to allow their effective enforcement in the digital environment. Accordingly, the international obligation to protect the right holder against acts of circumvention does not arise if the use of technological measures goes beyond the scope of the rights granted in the [WIPO Copyright Treaty] or the [Berne Convention].

*Id.*

It is debatable whether the same requirement of a link between the protection of technological measures and the protection of the rights granted by copyright applies in the EU to the protection of computer programs against "any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate . . . circumvention of any technical device which may have been applied to protect a computer program." Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, art. 7(1)(c), 2009 O.J. (L 111) 16.

[189] Copyright, Designs and Patents Act, 1988, c. 48, § 296ZF(3). The provision that applies to a person circumventing a technological measure "applied to a copyright work other than a computer program" is § 296ZA.

[190] "When speaking of 'acts which are not authorised' it is implicit that one is considering only acts which need authorisation, i.e. acts which are otherwise restricted. To 'authorise' a man to do something he is free to do anyway–something which needs no authority–is a meaningless concept." Lord Justice Jacob in *Neil Stanley Higgs v. The Queen*, [2008] EWCA (Crim) 1324, [32] (Eng.).

provides for technological protection measures.[191] Similarly, the German Copyright Act limits the protection provided to technological measures by defining them as measures that are "designed to prevent or restrict" unauthorized acts.[192] Therefore, the question of liability for circumvention of geolocation under the copyright laws of these countries depends on whether the cybertraveling user engages or may engage in an act of copyright infringement.[193]

Based on the territoriality principle that governs copyright laws, it would appear logical for acts of circumvention to be illegal under the laws that protect copyrighted works only if the acts are connected to the infringement of copyright under the law of the same country.[194] For example, if the associated act of direct

[191] However, for a discussion on copyright infringements that occur in the United Kingdom when temporary copies are created, see *infra* notes 220–21 and accompanying text.

[192] Gesetz über Urheberrecht und verwandte Schutzrechte [UrhG] [German Copyright Act], Sept. 9, 1965, Bundesgesetzblatt, Teil I [BGBl. I] 3044, as amended, § 108b(1) (Ger.); Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, art. 6(3), 2001 O.J. (L 167) 10, 17, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF.

[193] In a 2010 decision the German Supreme Court confirmed that technological measures are also protected by German law when they are designed to protect the right to make a work available to the public under §19a of the German Copyright Act. The right would probably not be interpreted to include the right of access by an individual user. *See* Bundesgerichtshof [BGH] [Federal Court of Justice] Apr. 29, 2010, MEDIEN, INTERNET UND RECHT [MIR] 159, 2010 (Ger.). For safeguards against technological measures that prevent uses allowed by copyright law see *infra* note 205. *See also Australian Copyright Act 1968* (Cth) § 10(1), *available at* http://www.adelaide.edu.au/legals/docs/copyright 1968.pdf ("[*C*]*ircumvention service* means a service, the performance of which has only a limited commercially significant purpose, or no such purpose or use, other than the circumvention, or facilitating the circumvention, of an [sic] technological protection measure."); Svantesson, *Cat and Mouse*, *supra* note 117, at 26–27 (discussing the technological protection measure provision of the Act).

[194] Theoretically, country A could impose liability under its copyright law even for a circumvention in country A of technological measures that was connected to an act of copyright infringement in country B. Courts in country A would then have to assess whether copyright was infringed under B's law. Courts in country A would determine liability for the acts of circumvention as long as A's courts considered copyright infringement actions to be transitory causes of action (meaning that infringements under B's copyright law would be justiciable in A's courts) or were willing to assess

copyright infringement is reproduction of the copyrighted work, the act of circumvention, if it can be tied to the direct infringement, can be infringing only where the act of reproduction occurred. Therefore, if a cybertraveler travels from Chile to Germany, and the only copyright infringing act that he commits is reproducing the accessed works on his computer in Chile (if the act is considered copyright infringing under Chilean law), it will be the Chilean anti-circumvention law that will apply; the German anti-circumvention provision will not apply if there is no associated act of copyright infringement that could be localized in Germany.[195]

The territorial limitations will not apply if a country's anti-circumvention provisions do not protect copyrighted works from access only for copyright infringing purposes but also for copyright non-infringing purposes. If the provisions are drafted to impose direct liability for *any* circumvention of measures that prevent access to the works—whether or not the circumvention occurs for the purpose of infringing copyright—no related act of copyright infringement in the same country will be necessary to find the user liable under the anti-circumvention provisions. Therefore, if country B has such anti-circumvention provisions, a user who cybertravels from country A to country B, or who cybertravels through servers located in country B on the way from country A to country C, may be liable in country B under the anti-circumvention provisions of country B even if while cybertraveling the user does not infringe copyright under the laws of country B.

In the United States, the federal circuits disagree on whether all of the provisions of the Digital Millennium Copyright Act ("DMCA") that protect technological measures[196] require a showing of nexus between the circumvention and the copyright

infringement under B's copyright law as an ancillary question. It appears unlikely that countries would be willing to extend their protection to foreign copyright laws, but if countries were willing to extend their protection to foreign copyright laws, a protective mechanism against enforcement of copyright laws that included policies contrary to A's policies could be drafted into A's anti-circumvention laws.

195 *See supra* notes 192–93 and accompanying text.

196 17 U.S.C. § 1201 (2006).

infringement.[197] The U.S. Court of Appeals for the Federal Circuit requires a plaintiff who complains of circumvention of its technological protection measures "to demonstrate that the circumventing technology infringes or facilitates infringement of the plaintiff's copyright."[198] This requirement means that the Federal Circuit's interpretation of the anti-circumvention provisions of the DMCA is consistent with the European approach because it limits liability under the provision to acts that result in copyright infringement;[199] other acts of circumvention that are not connected with existing or potential infringement are permitted.[200] In the cybertravel context this interpretation means that cybertravel, whether into the United States or from the United States, results in no liability under the DMCA unless there is an associated act of direct infringement that can be localized in the United States.[201]

[197] However, this circuit split may be irrelevant in practice because of the courts' approach to temporary copying and the possibility of rendering such copying as copyright infringing through a simple contractual provision. *See infra* note 224 and accompanying text.

[198] MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 948 (9th Cir. 2010) (citing Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004)). The *Chamberlain* court "conclude[d] that 17 U.S.C. § 1201 prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners. . . . [I]t is the only meaningful reading of the statute." Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1202–03 (Fed. Cir. 2004); *see also* Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307, 1319 (Fed. Cir. 2005) ("A court must look at the threat that the unauthorized circumvention potentially poses in each case to determine if there is a connection between the circumvention and a right protected by the Copyright Act.") (citation omitted).

[199] *Cf.* Bechtold, *supra* note 185, at 343, 390–92 (on options that EU member countries have when implementing provisions on protection of technological measures).

[200] *See Chamberlain*, 381 F.3d at 1204 ("A copyright owner seeking to impose liability on an accused circumventor must demonstrate a reasonable relationship between the circumvention at issue and a use relating to a property right for which the Copyright Act permits the copyright owner to withhold authorization—as well as notice that authorization was withheld."). *See also Storage Tech. Corp.*, 421 F.3d at 1318–19 (finding an insufficient nexus between the circumvention measure and rights protected by copyright law).

[201] *See infra* note 276 on "dual use" technologies.

The U.S. Court of Appeals for the Ninth Circuit disagrees with the Federal Circuit's interpretation of the anti-circumvention provisions of the DMCA.[202] The Ninth Circuit maintains, as does the Second Circuit,[203] that while section 1201(b) of the Copyright Act is bound to an act of copyright infringement, section 1201(a) creates liability for circumvention *per se*,[204] which means that an unauthorized act of circumvention leads to liability even if it is undertaken for purposes that are not copyright infringing.[205] The Ninth Circuit's interpretation therefore recognizes section 1201(a)

---

[202] *MDY Indus.*, 629 F.3d at 950.

[203] *See infra* note 208.

[204] Circumvention is illegal if it concerns any "technological measure that effectively controls access to a work." 17 U.S.C. § 1201(a)(1)(A) (2006).

[205] Among the arguments that the Ninth Circuit listed in support of its interpretation of section 1201(a) as prohibiting acts of circumvention of any measures controlling access to copyrighted work is the fact that section 1201(a) authorizes the Librarian of Congress to determine when circumvention for certain "noninfringing uses" of selected copyrighted works will be exempted from the provision. *See* 17 U.S.C. § 1201 (a)(1)(D) (2006); *MDY Indus.,* 629 F.3d at 951. The existence of the authorization to provide for exemptions suggests that absent an exemption, circumvention for "noninfringing uses" will result in liability under section 1201(a). Indeed, among the exemptions that the Librarian of Congress issued in July 2010 are examples of circumvention used to achieve what appear to be fair uses, such as circumvention of DVD Content Scrambling System to extract "short portions of motion pictures into new works for the purpose of criticism or comment . . . [for] educational uses by college and university professors." Libr. Of Cong., Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 75 Fed. Reg. 43825, 43827 (July 27, 2010) (codified at 37 C.F.R. § 201.40). However, similar fair-use-sounding uses appear among the "classes considered, but not recommended," *id.* at 43834, for which no exemption was issued. *See* 37 C.F.R. § 201.40 (2010). For instance, one of the classes that was not exempted in 2010 was "subscription based services that offer DRM-protected streaming video where the provider has only made available players for a limited number of platforms." Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 75 Fed. Reg. at 43834. In this case, the Librarian denied an exemption that would have allowed users to watch the video on other platforms, because alternative devices already exist (such as DVD players) that a user interested in a non-infringing use can utilize. *Id.* at 43835. Compare this with Copyright, Designs and Patents Act, 1988, c. 48, § 296ZE (detailing the complaint procedure and remedies available "where effective technological measures prevent permitted acts"). For other approaches that EU countries have adopted for the same problem of remedying protection by technological measures that affect copyright non-infringing uses see Bechtold, *supra* note 185, at 343, 392.

as creating a new "right to permit *access* to copyrighted work,"[206] a right that is not among the exclusive rights that copyright holders traditionally enjoy[207] and that is not—as opposed to the exclusive rights enumerated in section 106 of the Copyright Act—subject to the fair use doctrine.[208]

If the Ninth and Second Circuit Courts' interpretation of section 1201(a) prevails, cybertravel could expose a user to liability for the act of circumventing an access control, regardless of what use—copyright infringing or not—might follow, as long as there is access to a copyrighted work involved in the particular act of cybertravel and the court determines that geolocation tools are "effectively control[ling] access to a [copyrighted] work."[209] This interpretation has far-reaching consequences for cybertravel. Not only would the application of section 1201(a) result in liability for anyone cybertraveling from the United States, whether or not for copyright infringing purposes, but it would also lead to liability for anyone who cybertravels into the United States, regardless of purpose, or anyone who, through cybertravel to another country, accesses a website stored on a server in the United States, regardless of purpose. In any of these cases, under the Ninth and Second Circuit's interpretation, a breach of section 1201(a) would

---

206 It could also be called the right to prevent digital trespass.

207 On the relevant legislative history see *MDY Indus.*, 629 F.3d at 946 ("Congress created a new anticircumvention right in § 1201(a)(2) independent of traditional copyright infringement and granted copyright owners a new weapon against copyright infringement in § 1201(b)(1)."); *id.* at 948 ("[S]ection (a) creates a new anticircumvention right distinct from copyright infringement, while section (b) strengthens the traditional prohibition against copyright infringement."). *See also* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 441 (2d Cir. 2001) (identifying the distinction between sections (a) and (b)).

208 *See* 17 U.S.C. §107 (2006). *See also Universal City Studios*, 273 F.3d at 443 (rejecting the argument that circumvention of encryption technology protecting copyrighted material should be exempt[ed] from copyright liability "when the material will be put to 'fair uses.'"). In the same case the appellants unsuccessfully attempted to present a constitutional argument. *Id.* at 444–45. *See also* Gideon Parchomovsky & Philip J. Weiser, *Beyond Fair Use*, 96 CORNELL L. REV. 91, 103–04 (2010) (discussing the *Universal City Studios* case); *id.* at 93 (arguing that, "[t]he golden era of fair use—if one ever existed—ended . . . with the enactment of the Digital Millennium Copyright Act").

209 17 U.S.C. §1201(a)(3)(B) (2006). For a discussion of the requirement of "effectiveness" of technological measures see *supra* note 185.

occur because the use of the cybertravel tools would occur in the United States.[210]

The only way to remove any cybertravel to, from, or through the United States from the application of the DMCA as interpreted by the Ninth and Second Circuit Courts would be to achieve an exemption from the Librarian of Congress from the scope of the anti-circumvention provision;[211] whether such an exemption is possible depends, *inter alia*, on whether the cybertravel is being employed for copyright non-infringing purposes.[212] Whether the acts in which the user engages through cybertravel are infringing or non-infringing is decisive if the interpretation by the Federal Circuit is adopted, and an analysis of the user's possible direct copyright infringement liability under potentially applicable foreign laws is essential in determining whether the user who travels into or through the United States may also be directly liable for circumvention of technological protection measures in the foreign country of direct infringement.

The viewing of a copyrighted work does not *per se* infringe copyright. Once a work is made available to the public any user is free to view a work even without the copyright holder's authorization unless a "right to permit access to [the] copyrighted work" exists, which may be the case under the interpretation by the Ninth and Second Circuits of section 1201(a) of the Copyright Act. However, reproducing a work without authorization may be an act of copyright infringement, and therefore if a cybertraveler (or any Internet user, for that matter) deliberately makes a copy of a work, absent a valid defense or copyright exception, the cybertraveler will be liable for copyright infringement.[213] The problem is that

---

[210] For a discussion of such a scenario, see *supra* note 194 and accompanying text.

[211] For a discussion of the exemption process, see *supra* note 205.

[212] 17 U.S.C. §1201(a)(1)(D) (2006).

[213] Here some significant differences exist between the United States and the rest of the world because outside the United States users do not enjoy as many limitations on the rights conferred by copyright as users in the United States enjoy under the U.S. fair use doctrine. Generally, other countries rely on a limited number of enumerated exceptions to copyright. *See, e.g.*, Amélie Blocman, *Court of Cassation Pronounces on Private Copying Versus Technical Protective Devices*, IRIS Merlin 2006-4:12/20, *available at* http://merlin.obs.coe.int/iris/2006/4/article20.en.html (last visited Nov. 19, 2011)

even if the user only intends to view the work without creating a copy, a copy is created anyway—automatically, by the user's computer memory in the process of displaying the work. The question then becomes whether this copying in a computer's temporary memory, which occurs outside a user's control,[214] is an infringing reproduction as defined by copyright law,[215] and if so, whether it falls within one of the exceptions to copyright, or is subject to the fair use doctrine.[216]

Existing court decisions suggest that the status of temporary copies will depend, *inter alia*, on the associated acts by the user.[217] As long as the temporary copies are made in the course of a lawful use of the work they will likely be non-infringing; however, if they are created as a part of an unlawful use, they may be held infringing. In the United States, the Ninth Circuit in *Perfect 10, Inc. v. Amazon.com, Inc.*[218] explained that the creation of temporary copies on a user's computer may constitute fair use in a particular situation, but the court indicated that not every temporary copy will be fair use.[219] U.K. courts have declared

(discussing a case involving circumvention of technological protection measures for purposes of creating a private copy).

[214] *See, e.g.*, Jesse S. Bennett, *Caching In On the Google Books Library Project: A Novel Approach to the Fair Use Defense and the DMCA Caching Safe Harbors*, 35 FLA. ST. U. L. REV. 1003, 1007–22 (2008) (discussing temporary, transient, and cache copies).

[215] *See* Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121, 127 (2d Cir. 2008) (on buffer data as not being copies under the U.S. Copyright Act); Ticketmaster L.L.C. v. RMG Tech., Inc., 507 F. Supp. 2d 1096, 1105–06 (C.D. Ca. 2007) (on cache copies as copies under the U.S. Copyright Act).

[216] *See generally* Aaron Perzanowski, *Fixing RAM Copies*, 104 NW. U. L. REV. 1067 (2010) (discussing the development of the legal status of RAM copies). On temporary copies and streaming see generally Frank A. Koch, *Der Content bleibt im Netz – gesicherte Werkverwertung durch Streaming-Verfahren*, 7 GRUR 574 (2010); Borghi, *supra* note 24 (exploring the copyright implications of the use of on-demand and live streaming technologies in the context of European case law).

[217] There are several issues involved in decisions on temporary copies; a detailed analysis of all of the issues is beyond the scope of this article. *See supra* note 14 and accompanying text (generally commenting on the scope of this article).

[218] Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

[219] *Id.* at 1169.

> [E]ven assuming such automatic copying could constitute direct infringement, it is a fair use *in this context*. The copying function performed automatically by a user's computer to assist in accessing

automatically-created temporary copies to be infringing when the copies resulted from playing counterfeit video games;[220] these copies could not benefit from the explicit exception from copyright protection that temporary copies enjoy under the U.K. law because the exception applies only if such copies are created to enable "a lawful use of the work" with "no independent economic significance."[221]

The "lawfulness" of the use of a copyrighted work does not depend only on the status of the acts under copyright law; the use of a work will be "unlawful" even if it is contrary only to a provision in a user agreement.[222] Therefore, for instance, if a user agreement limits possible uses to non-commercial purposes, using the work for commercial purposes will be unlawful, and any temporary copying associated with the commercial purposes may

> the Internet is a transformative use. Moreover, . . . a cache copies no more than is necessary to assist the user in Internet use. It is designed to enhance an individual's computer use, not to supersede the copyright holders' exploitation of their works.

*Id*. (emphasis added).

*Compare* Ticketmaster, LLC v. RMG Tech., Inc., 507 F .Supp. 2d 1096, 1109–10 (C.D. Cal. 2007) (discussing the status of cache copies), *with* Cartoon Network LP, LLLP v. CSC Holding, Inc., 536 F.3d 121 (2d Cir. 2008). In *Cartoon Network*, the Second Circuit distinguished between buffer data and "data . . . embodied in the computer's RAM memory until the user turned the computer off." *Id*. at 130. The Court held that buffer data did not fulfill the fixation or embodiment requirement under copyright law, specifically the duration requirement. *Id*. at 127, 130.

[220] Sony Comp. Entm't v. Ball, [2004] EWHC (Ch) 1738, 6 [15], (Eng.); R v. Higgs, [2008] EWCA (Crim) 1324 (Eng.); R v. Gilham, [2009] EWCA (Crim) 2293 [25] (Eng.) ("[E]ven if the contents of the RAM of a game console at any one time is not a substantial copy, the image displayed on screen is such.").

[221] Copyright, Designs and Patents Act, 1988, c. 48, § 28A(b) (Eng.). The second exception is made to enable "a transmission of the work in a network between third parties by an intermediary." Copyright, Designs and Patents Act, 1988, c. 48, § 28A(a) (Eng.); *see also* Copyright, Designs and Patents Act, 1988, c. 48, § 17(6) (Eng.) (explaining that infringing "copying in relation to any description of work includes the making of copies which are transient or are incidental to some other use of the work"). On the situation under German law see Koch, *supra* note 216; Thomas Busch, *Zur urheberrechtlichen Einordnung der Nutzung von Streamingangeboten*, 6 GRUR 496, 501–03 (2011).

[222] However, under the WIPO Copyright Treaty countries are not required to protect technological measures designed to protect a work beyond the protection afforded by copyright. *See* WIPO Copyright Treaty, *supra* note 184, at art. 11.

be considered infringing.[223] The fact that an appropriately worded user agreement may render temporary copies infringing[224] means in practice that the difference in the approaches to § 1201(a) taken by the Federal Circuit and the Ninth and Second Circuits might be marginal: the terms of the user agreement could cause courts to view the creation of any temporary copies as a violation of the user agreement, and the user could be subject to liability under § 1201(a) for an act of circumvention associated with the creation of such copies even under the Federal Circuit's "European-style" interpretation.

Whether a user breached a user agreement will affect a user's liability for circumvention only when the user cybertravels *from* the United States; it will have no effect on a user's liability if the user cybertravels *into* the United States. The user cybertraveling from Chile to the United States to access a copyrighted work will be liable under the Ninth and Second Circuits' interpretation of §

---

[223] This conclusion appears to be confirmed by the decision in Newspaper Licensing Agency Ltd. v. Meltwater Holding BV, [2010] EWHC (Ch) 3099 (Eng.).

> [T]he temporary copies exception is solely concerned with incidental and intermediate copying so that any copy which is 'consumption of the work', whether temporary or not, requires the permission of the copyright holder. A person making a copy of a webpage on his computer screen will not have a defence under s. 28A CDPA simply because he has been browsing. He must first show that it was lawful for him to have made the copy. The copy is not part of the technological process; it is generated by his own volition. The whole point of the receipt and copying of Meltwater News is to enable the End User to receive and read it. Making the copy is not an essential and integral part of a technological process but the end which the process is designed to achieve.

*Id.* at [109].

> The exception cannot have been intended to legitimise all copies made in the course of browsing or users would be permitted to watch pirated films and listen to pirated music. The kind of circumstance where the defence may be available is where the purpose of the copying is to enable efficient transmission in a network between third parties by an intermediary, typically an internet service provider.

*Id.* at [110]; *see also* Newspaper Licensing Agency Ltd. & Ors v. Meltwater Holding BV & Ors, [2011] EWCA Civ 890 (Eng.), at [30]-[35].

[224] *See, e.g.*, Ticketmaster, LLC v. RMG Tech., Inc., 507 F .Supp. 2d 1096, 1110 (C.D. Cal. 2007) (finding cache copying was not fair use if it occurred while the defendant violated the Terms of Use).

1201(a), regardless of whether or not he accessed the content in breach of a user agreement, because the Ninth and Second Circuits do not require a related act of copyright infringement in the United States to accompany the circumvention of technological measures. The existence or non-existence of a user agreement will also have no effect on the result of the assessment of the user's liability under the Federal Circuit's interpretation in a scenario in which the user cybertravels into the United States, but with the opposite result: the user should not be liable in the United States under § 1201(a) of the DMCA because the temporary copy created by the user's computer in Chile does not infringe U.S. copyright law (though it may infringe Chilean law if Chilean law considers infringing the creation of temporary copies that result from an unlawful use of a work). The only scenario in which a breach of a user agreement will make a difference is when a user cybertravels *from* the United States and the Federal Circuit's interpretation of § 1201(a) of the DMCA is operative: without a user agreement the user's cybertravel for purposes that do not infringe copyright will be legal because the temporary copies on his computer will not violate a user agreement, but under a user agreement that renders temporary copies copyright infringing, cybertravel will be illegal.[225]

b) Liability under Other Laws

User agreements may not only generate or solidify right holder protection under copyright law provisions on protection of technological measures, but the agreements, if breached, may also expose end users to contractual liability.[226] To limit cybertravel directly under contract, content providers may prohibit users from changing the information that identifies their physical location.

[225] Under the Ninth and Second Circuit's interpretation of section 1201(a) the breach of a user agreement will not matter, whether a user cybertravels from or into the United States: all cybertravel will violate the anti-circumvention provisions of section 1201(a).

[226] "Contract law has rapidly become a regular companion to copyright protection as the structure of the Internet enables the formation of contract relationships between information producers and end users, either directly or through intermediaries." PAUL GOLDSTEIN & P. BERNT HUGENHOLTZ, INTERNATIONAL COPYRIGHT: PRINCIPLES, LAW, AND PRACTICE 334 (Oxford University Press, 2d ed. 2010).

For instance, the German television station SAT1 in its user agreement includes a provision against circumvention of the geographical limitations that SAT1 imposes on access to audiovisual content on its website.[227] According to the agreement, the user must "use the retrieved content only within the use areas permitted by [the media company], and may not in particular alter, circumvent or otherwise disregard technical measures applied by [the media company] to territorially limit the use."[228] Consequently, users cybertraveling from unpermitted areas breach the contract and are exposed to direct liability through the contractual provisions; the applicable law in user agreements like that of SAT1 will often be set in the contract, or may depend on choice-of-law provisions in the country where the cybertraveler is sued.

Because cybertravel entails remote access to content stored on a computer or a storage facility,[229] the question arises as to whether cybertravel can expose users to liability under anti-hacking laws, and not only to civil but also to criminal liability. Anti-hacking provisions such as the Computer Fraud and Abuse Act in the United States[230] target acts of access to a computer without authorization,[231] and such acts include not only physical access but

---

[227] *Nutzungsbedingungen für die Nutzung des Videoportals von Sat.1* [Terms and Conditions for Use of the Sat.1 Video Portal], SAT.1, http://www.sat1.de/service/nutzungsbedingungen/nutzungsbedingungen-fuer-die-nutzung-des-videoportals-von-sat-1 (last visited Nov. 11, 2011) (Ger.).

[228] *Id.* § 4.1(g) (English translation).

[229] Data storage facilities are included in the definition of a "computer" in the Computer Fraud and Abuse Act. 18 U.S.C. § 1030(e)(1) (2008); *see also*, Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, art. 1(a), 2005 O.J. (L 69) 48 (EU); Computer Misuse Act, 1990, c. 18, § 17(6) (Eng.). The definition is likely to expand to encompass a greater number of devices; for instance, recently the U.S. Court of Appeals for the Eighth Circuit confirmed that a cellular phone is a "computer" under the provision. *See* United States v. Kramer, 631 F.3d 900, 901 (8th Cir. 2011). For a discussion of "access," see Computer Misuse Act, 1990, c. 18, § 17(2) (Eng.).

[230] *See* 18 U.S.C. § 1030.

[231] *E.g.*, *id.* § 1030(a)(2)(C) ("Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . ."); *see also* Council Framework Decision 2005/222/JHA of 24

also remote access through a network.[232] However, there could be limitations on the liability of a cybertraveler under anti-hacking provisions; for instance, under U.S. law a cybertraveler's acts might not result in the kind of "damage"[233] or "loss"[234] that would warrant a civil action against the cybertraveler.[235] Perhaps the website operator could avoid this limitation by permitting access to restricted content only for a fee;[236] cybertraveling to the United States to avoid the fee would then bring the cybertraveler within

February 2005 on attacks against information systems, art. 2(1), 2005 O.J. (L 69) 48 (EU); Computer Misuse Act, 1990, c. 18, §§ 1(1), 17(5), 17(8) (Eng.).

[232] 18 U.S.C. § 1030(a); *see also*, Council of Europe Convention on Cybercrime, Budapest, November 23, 2001, ch. 2 § 1 art. 2, *available at* http://conventions.coe.int /Treaty/en/Treaties/html/185.htm; Council Framework Decision 2005/222/JHA, *supra* note 231, art. 1(d); Computer Misuse Act, 1990, c. 18, § 1(1) (Eng.).

[233] The Computer Fraud and Abuse Act defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). For a discussion of the terms "damage" and "loss" under the Act see, e.g., Multiven, Inc. v. Cisco Sys., 725 F. Supp. 2d 887, 894–95 (N.D. Cal. 2010).

[234] According to the Computer Fraud and Abuse Act,

> "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(e)(11).

[235] *Id.* § 1030(g).

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i) . . . .

*Id.* The only potentially relevant factor would be

> loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value . . . .

*Id.* § 1030(c)(4)(A)(i)(I); *see also* EU Council Framework Decision 2005/222/JHA, *supra* note 231, at art. 2(1) (allowing EU member states not to criminalize certain acts of accessing information systems in cases that are considered "minor").

[236] This solution addresses only the issue of the magnitude of the loss; it does not address the potential problem of the nature of the loss as defined in 18 U.S.C. § 1030(e)(11).

the scope of the Act.[237] Although making access from abroad contingent upon the payment of a fee might be a straightforward and simple solution to implement technically, it might not always be possible; in many cases website operators employ geolocation tools because they either do not have rights to make the content available to users from certain countries or they do not want to be regulated by the laws of those countries.[238]

Although allowing access from countries from which access is restricted, even for a fee, might not always be an option, one business implementation on the horizon may test this arrangement. The BBC announced in November 2010 its plan to offer to users connecting to its website from outside the United Kingdom some of the content that it currently makes available only to users connecting from inside the United Kingdom.[239] Making access from abroad contingent upon the payment of a fee while maintaining free access for users connecting from inside the United Kingdom could result in liability not only for users who cybertravel to avoid payment of the fee but also for those who facilitate the cybertravel to the United Kingdom by providing the tools that enable the cybertravel. Apart from making applicable various legal doctrines to prevent unwanted cybertravel, such a pay-per-foreign-view system will compete with the services of mainstream cybertravel providers who charge for their tools that are designed to accomplish the same result—the viewing of the restricted foreign content. The next section analyzes the question of liability of cybertravel providers, whether or not those using their tools circumvent a fee when cybertraveling.

---

[237] *See infra* note 246 and accompanying text for a further discussion of how making content available for a fee might bring a cybertravel provider within the scope of not only the Computer Fraud and Abuse Act in the United States but also national provisions implementing the 1998 EU Conditional Access Directive.

[238] *See supra* Part II.A for a discussion of the reasons for using geolocation tools to limit access to content.

[239] Jonathan Wynne-Jones, *BBC Aims to Gain from Global iPlayer*, TELEGRAPH (Nov. 7, 2010), http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/8114911/BBC-aims-to-gain-from-global-iPlayer.html.

2. Liability of Cybertravel Providers

Although individual cybertravelers may be subject to direct liability in either the country where they are physically located or the country to which they cybertravel, they might not be the best targets for enforcement actions; as has been shown in the relatively short history of the Internet, the most valuable enforcement targets are often intermediaries. Enforcement actions against individual Internet users can be highly inefficient, and the costs of detection and enforcement will often be excessive when compared to any benefits that might be achieved through such enforcement—both in terms of recourse against individual users and the deterrence of other users;[240] enforcement against intermediaries is likely to yield better results. In the case of cybertravel these intermediaries are the providers of cybertravel tools.

Cybertravel providers should be concerned about the secondary liability they might face in connection with end users who use their cybertravel tools for direct infringement;[241] however, providers might also need to be concerned about exposing themselves to direct liability. For example, in the case of South Africa, it is possible that cybertravel providers could be held liable as "persons, entities or organisations which facilitate the provision of [illegal] on-line gambling."[242] Cybertravel providers could also face direct liability under copyright law provisions that protect technological measures; national implementing provisions concerning the measures cover acts of manufacturing, importation, offering to the public, providing, and otherwise trafficking in technologies for circumventing technological measures.[243] For providers to be liable, some nexus will generally be required between the acts of facilitated circumvention and potential or

[240] For a discussion of the problem of "asserting control at the source" see Zittrain, *supra* note 116, at 207–09. *See also* Goldstein & Hugenholtz, *supra* note 226, at 330–31.

[241] *See infra* for a discussion of the potential indirect liability of cybertravel providers.

[242] *On-line Gambling Transactions Are Outlawed in South Africa*, GAUTENG GAMBLING BD., http://www.ggb.org.za/index.php?option=com_content&view=article&id=3:newsflash-2&catid=3:newsflash (last visited Nov. 19, 2011).

[243] *E.g.*, 17 U.S.C. § 1201(a)(2), (b)(1) (2006). While the Federal Circuit Court views these DMCA provisions as codifying forms of secondary liability, the provisions are drafted to create direct liability.

existing copyright infringement.[244] However, in the United States no nexus is required if the Ninth and Second Circuits' interpretation of section 1201(a) applies, and cybertravel providers may be liable for providing circumvention tools even without a nexus.[245]

Cybertravel providers face another problem if their tools allow users to bypass the payment of a fee for access. As explained earlier,[246] website operators can decide to provide content for free in countries where access is not restricted but charge a pay-per-foreign-view fee to users accessing the same programming from other countries. If cybertravel providers facilitate user access to websites without the payment of a required fee, the providers could be exposed in the United States to liability under the Computer Fraud and Abuse Act,[247] and similarly, in the EU, the providers could be liable under national provisions implementing the 1998 EU Conditional Access Directive,[248] which protects services that limit access in order to collect remuneration[249] from "illicit devices which allow access to these services free of charge."[250] Infringing activities under the Directive include the manufacture, import, distribution, sale, rental, possession, installation, maintenance,

[244] It is debatable whether the same nexus is required in the EU for the protection of computer programs against "any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate . . . circumvention of any technical device which may have been applied to protect a computer program." Council Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, art. 7(1)(c), 2009 O.J. (L 111) 52.

[245] *See supra* Part IV.A.1.a (discussing the circuit split).

[246] *See id.*

[247] *See supra* text accompanying notes 230–35; *see also* 18 U.S.C. §1030(a)(6)(A) (2008).

[248] Directive 98/84 of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, 1998 O.J. (L 320) 54 [hereinafter 1998 EU Conditional Access Directive]; *see also* European Convention on the Legal Protection of Services Based on, or Consisting of, Conditional Access, COUNCIL OF EUROPE (Jan. 24, 2001), http://conventions.coe.int/Treaty/en/Treaties/html/178.htm.

[249] 1998 EU Conditional Access Directive, *supra* note 248, at recitals 3, 6.

[250] *Compare* 1998 EU Conditional Access Directive, *supra* note 248, at recital 6 *and* 47 U.S.C. § 605 (2006) (unauthorized publication or use of communications), *with* 47 U.S.C. § 553 (2006) (unauthorized reception of cable service).

replacement and use for commercial purposes[251] of "any equipment or software designed or adapted to give access to a protected service."[252]

Even if their cybertravel tools are not used to bypass the payment of a fee, cybertravel providers should be concerned about their liability under anti-hacking provisions. These provisions target not only hackers but also those who provide tools for hacking, such as "any password or similar information through which a computer may be accessed without authorization."[253] Cybertravel tools could be viewed as such "similar information," and therefore, tool providers could face civil and criminal liability under anti-hacking laws, subject to the limitations mentioned above that are applicable to cybertravelers.[254] Additionally, limitations associated with territoriality may exist in countries where the liability of providers of hacking tools is drafted in the form of secondary liability.

Another danger for cybertravel providers is direct liability for secondary transmission. Other services that resemble cybertravel have been designed to "place shift," or to facilitate the viewing of content elsewhere that is broadcast or made available to a limited geographical area, and some of these similar services have been challenged based on their retransmission of the content. For instance, in Japan a service called ManekiTV offered "a location-free, Internet-based transmission" of Japanese television programs for a fee;[255] in January 2011 the Supreme Court of Japan held that the service infringed copyright.[256] In the United States, a similar

---

[251] 1998 EU Conditional Access Directive, *supra* note 248, at art. 4.

[252] *Id.* at art. 2(e).

[253] 18 U.S.C. §1030(a)(6) (2008). Under national provisions that implement Article 5 of EU Council Framework Decision 2005/222/JHA in the EU member states, such tool providers could be criminally liable. *See* Council Framework Decision 2005/222/JHA of the European Union of 24 February 2005 on attacks against information systems, 2005 O.J. (L 69) 67, 69. For limitations on liability under that legislation, see *supra* notes 233–35 and accompanying text. *See also* Computer Misuse Act, 1990, c. 18, § 3A (Eng.).

[254] *See supra* notes 230–35 and accompanying text.

[255] Aritake, *supra* note 23; *see also* MANEKITV, *supra* note 19.

[256] *See* Aritake, *supra* note 23.

service has been attacked in *WPIX, Inc. v. ivi, Inc.*.[257] ivi's online TV player allows users to view on the Internet broadcasts that were originally available over the air.[258] In February 2011, the Federal District Court for the Southern District of New York issued a preliminary injunction against ivi, Inc.,[259] determining that the service is not eligible for the statutory license established by the U.S. Copyright Act for cable services.[260]

It may be argued that there is an important difference between place shifting services and cybertravel. While the technologies employed by ManekiTV and ivi require that the services retransmit the signal to provide access to additional viewers, cybertravel technologies, with one exception, do not involve the retransmission of a signal. Instead of retransmitting a signal, cybertravel tools relocate the user in cyberspace so that the user can access the content directly from the original website. The tools do not retransmit the content; rather, they "shift" the perceived location of the viewer. The one exception might be website cybertravel tools—websites that display web pages based on users' requests. These tools could be described as operating on the principle of retransmission; however, as noted earlier, this type of tool is unlikely to be utilized for content streaming because it involves slow connection speeds.[261]

---

[257] WPIX, Inc. v. ivi, Inc., 765 F. Supp. 2d 594 (S.D.N.Y. 2011).

[258] IVI, *supra* note 16.

[259] *WPIX, Inc*., 765 F. Supp. 2d at 622. Other services, such as Slingbox, a U.S. service that allows users to "[w]atch and control [their] TV shows over the Internet from anywhere in the world," could face similar challenges depending on their particular technology. SLINGBOX, http://www.slingbox.com/go/slingbox (last visited Feb. 2, 2012). The Slingbox concept is similar to the bypassing of geolocation that is described in Part III of this paper as "self-sustained" cybertravel because Slingbox also requires a user's own device (the Slingbox) located in another country. A similar service in Japan is Rokuraku. *See* H. Kikuchi, *Comment on the Rokuraku II decision*, 41 INT'L REV. INTELL. PROP. & COMPETITION L. 860 (2010)*; see also* ROKURAKU, http://www.rokuraku.com/ (last visited Nov. 19, 2011).

[260] 17 U.S.C §111(c)(1) (2006). The Register of Copyrights has proposed that the provision be phased out. *Satellite Television Extension and Localism Act*: Section 302 Report, REGISTER OF COPYRIGHTS (Aug. 29, 2011), http://www.copyright.gov/reports/section302-report.pdf. For additional examples see, *supra* notes 16–21 and accompanying text.

[261] *See supra* Part III.

Although the phrase "making available" that is used in the 1996 WIPO Copyright Treaty and the 2001 EU Information Society Directive might seem to capture the involvement of cybertravel providers in the acts of cybertravel better than retransmission, public performance, or public display,[262] "making available" might not cover cybertravel providers' conduct. The right to communicate a copyrighted work to the public in Article 8 of the 1996 WIPO Copyright Treaty and Article 3 of the 2001 EU Information Society Directive[263] indeed includes the component of "making available to the public."[264] However, the Agreed Statement Concerning Article 8 of the WIPO Copyright Treaty suggests that the component does not create specific liability for passive behavior,[265] and explains that Article 8 does not impose liability for acts of "mere provision of physical facilities for enabling or making a communication." Similarly, recital 23 of the 2001 EU Information Society Directive states that the right "should cover any . . . transmission or retransmission of a work to the public" and that the "right should not cover any other acts."[266] The Directive is different from the WIPO Treaty in that, with respect to holders of rights to specific subject matter in Article 3(2),[267] the Directive *does* appear to create a new "right to make

[262] 17 U.S.C. §§ 106(4)–(5) (2006); *see also* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1159 (9th Cir. 2007).

[263] *See* 2001 EU Information Society Directive, *supra* note 187, at art. 3; Case C-306/05, Sociedad General de Autores y Editores de España (SGAE) v. Rafael Hoteles SA, 2006 E.C.R. I-11519.

[264] WIPO Copyright Treaty art. 8, Dec. 20, 1996, S. TREATY DOC. NO. 105-17, 36 I.L.M. 65, 70 (1996); 2001 EU Information Society Directive, *supra* note 187, at art. 3.

[265] The phrase is used to clarify the scope of the term "public." "[T]he making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them." WIPO Copyright Treaty art. 8, Dec. 20, 1996, S. TREATY DOC. NO. 105-17, 36 I.L.M. 65, 70 (1996). *See also* the definition of performing or displaying a work "publicly" in 17 U.S.C. §101 (2006) (providing the definition of performing or displaying a work "publicly"); Goldstein & Hugenholtz, *supra* note 226, at 328–29.

[266] 2001 EU Information Society Directive, *supra* note 187, at recital 23.

[267] The "exclusive right to authorize or prohibit the making available to the public" is provided to

> performers, of fixations of their performances; . . . for phonogram producers, of their phonograms; . . . for the producers of the first

available to the public," which "cover[s] all acts of making available such subject-matter to members of the public,"[268] meaning acts that are not restricted to transmission or retransmission.[269] However, the Directive repeats that "[t]he mere provision of physical facilities for enabling or making a communication does not in itself amount to communication,"[270] leaving open the question of whether providing cybertravel tools is equivalent to providing "facilities" and thus exempted from liability under the "making available" provision of the Directive.[271] In the United States, cybertravel providers might benefit from an exemption that passive carriers enjoy from liability for the "secondary transmission of a performance or display of a work."[272]

Indirect liability may be limited by safe harbor provisions that protect Internet intermediaries from secondary liability for Internet users' conduct; the provisions may also apply to cybertravel providers.[273] Safe harbor provisions apply to Internet service

> fixations of films, of the original and copies of their films; . . . for broadcasting organization, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.

2001 EU Information Society Directive, *supra* note 187, at art. 3(2).

[268] *Id.* at recital 24.

[269] On conflicting European decisions concerning hyperlinks, see Bechtold, *supra* note 185, at 343, 361.

[270] 2001 EU Information Society Directive, *supra* note 187, at recital 27.

[271] It speaks in favor of such an interpretation that recital 25 of the Directive seems to suggest that Article 3(2) should target on-demand transmission services. 2001 EU Information Society Directive, *supra* note 187, at recital 25. However, recital 23 of the Directive calls for a broad interpretation of the right. *Id.* at recital 23. *See also* Case C-306/05, Sociedad General de Autores y Editores de España (SGAE) v. Rafael Hoteles SA, 2006 E.C.R. I-11519, at par. 36. In *ITV v. TV CatchUp Ltd*., Justice Floyd opined that TV CatchUP does not "*merely* provide technical means to ensure or improve reception . . . It is not merely supportive of the original exploitation of the work." *ITV v. TV CatchUp Ltd.* [2011] EWHC 1874 (Pat), [98]. *See also* Bechtold, *supra* note 185, at 343, 361. As Goldstein and Hugenholtz note, "[p]osting hyperlinks to works already available on websites, however, is not an independent act of communication." Goldstein & Hugenholtz, *supra* note 226, at 329–30.

[272] 17 U.S.C. § 111(a) (2010).

[273] *E.g.*, *Id.* § 512; Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, arts. 12–15, 2000 O.J. (L 178).

providers without regard to the location of users who connect to their networks; therefore, in the case of the most basic cybertravel, which consists of a dial-up connection to a foreign Internet service provider,[274] the fact that the user connects from another country should not defeat the safe harbor that the service provider enjoys. Even cybertravel providers that are not Internet service providers can probably benefit from the provisions of the safe harbors that are designed for transitory digital network communications.[275]

Not all countries offer safe harbor provisions for Internet intermediaries, and even those countries that do offer safe harbor provisions may limit their safe harbors to secondary liability for infringements of only certain laws. Moreover, the safe harbor provisions will certainly not protect cybertravel providers from liability for actively inducing infringements. To limit their indirect liability, cybertravel providers will likely market their tools in a manner that does not suggest that they are promoting copyright infringement or other rights infringement by end users.[276] For instance, instead of advertising that their tools will allow users to watch specific copyrighted content, the providers may choose nonspecific language to advertise the fact that their tools may enable users to watch television programs in general.[277]

Cybertravel providers may also attempt to limit their exposure to indirect liability by disassociating their activities from the countries from which users, who use their tools, cybertravel.[278]

---

[274] *See supra* Part III.

[275] *E.g.*, 17 U.S.C. §512(a); Directive 2000/31/EC, *supra* note 273, at art. 12 ("Mere conduit").

[276] On the "dual use" technologies that may serve both legal and illegal purposes see Stefan Bechtold, *supra* note 185, at 343, 387. "In general, in such 'dual use' cases, [the provision on protection of technological measures] probably applies as long as the technological measure is not misused primarily for the purpose to substitute the absence of copyright protection by technological protection." *Id.* at 387; *see also* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, 545 U.S. 913, 936–41 (2005).

[277] *E.g.*, MY EXPAT NETWORK, *supra* note 150 (Note: the U.K. top-level domain name, the price in British pounds, the website strictly addressing British expatriates living outside the United Kingdom, and the language about watching "UK TV abroad.").

[278] *See* Martin Senftleben, commentary on the 1996 WIPO Copyright Treaty, *in* CONCISE EUROPEAN COPYRIGHT LAW 87, 102–03; *see also* Bechtold, supra note 185, at 343, 362.

Although the likelihood of success of such attempts is questionable, it is instructive to review their model.[279] For example, a cybertravel provider in Hungary might offer a cybertravel tool to Hungarians who travel abroad and wish to view Hungarian programs online that are not accessible outside of Hungary. The provider could argue that because any acts of potential direct copyright infringement would be committed by users outside Hungary, and therefore under foreign (non-Hungarian) copyright laws, no indirect liability of the cybertravel provider for copyright infringement should arise in Hungary under Hungarian law. Of course, the provider would also claim that it had not directed its operations at the countries in which acts of direct infringement occur (all countries other than Hungary), but only at Hungary, and thereby attempt to limit its exposure to personal jurisdiction outside Hungary.[280] Indeed, a provider could support its claim if its website were in Hungarian, as that would suggest that it had only targeted customers inside the sole country in which Hungarian is widely spoken and understood.[281]

Although existing laws do not address cybertravel, a number of legal doctrines may apply to various aspects of cybertravel, and it is for the courts to decide which, if any, of these existing doctrines apply. The lack of any specific legislative provisions addressing cybertravel is not surprising given the brief history of the use of geolocation tools to limit access to certain content and the relatively recent advent of cybertravel. So far there appear to be no cases raising the question of the legality of cybertravel, whether in the context of copyright law or of other laws pertaining to conduct on the Internet. Whether or not courts decide to deem

---

279 *See supra* note 277.

280 One could be found secondarily liable for copyright infringement in the country where direct infringement occurred. *E.g.*, Columbia Pictures Ind., Inc. v. Gary Fung, No. CV 06-5578 SVW (JCx), 2009 WL 6355911, at *18 (C.D. Cal. Dec. 21, 2009); Armstrong v. Virgin Records, Ltd., 91 F. Supp. 2d 628, 634–37 (S.D.N.Y. 2000).

281 *See* Joined Cases C-585/08 & C-144/09, Peter Pammer v. Reederei Karl Schluter GmbH & Co KG *and* Hotel Aplenhof GesmbH v. Oliver Heller (2010), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008CJ0585:EN:HTML (describing the European Union's treatment of websites for purposes of personal jurisdiction).

cybertravel legal under existing laws, it is time to discuss the future of cybertravel.

### *B. Should Cybertravel be Legal?*

Although current legal regimes do not directly address cybertravel and court cases dealing with cybertravel appear to be nonexistent, it would be a mistake to think that cybertravel will continue to remain outside the scope of legal inquiry.[282] The need to erect borders on the Internet to prevent the undesirable results of the application of cyberlaw 2.0[283] seems to dictate only one possible future for cybertravel: making it illegal. Without making or keeping cybertravel illegal, the goal of those who want a territorial partitioning of the Internet will be defeated or significantly endangered. Therefore it seems that, regardless of its current status, it is imperative that cybertravel be declared illegal.[284] This section discusses the apparently grim and inevitable fate of cybertravel and then attempts to identify potential arguments for saving it.

#### 1. Cybertravel as a Misrepresentation of One's True Location

There currently exists no right to know a user's true IP address, and no corresponding obligation for a user to reveal his true IP address; however, this could change in light of the developments outlined above.[285] The developments appear to dictate that in the future a user's IP address be unchangeable; if that be the case, an IP address will constitute an element of a user's digital identity that the user would not be permitted to alter. The user would have a

---

[282] *Cf.* Yvette Joy Liebesman, *The Wisdom of Legislating for Anticipated Technological Advancements*, 10 J. MARSHALL REV. INTELL. PROP. L. 154, 157 (2010) (warning that "we should proceed with caution in allowing the potential effects of either technology in its infancy or future unrealized technology to influence our policy decisions before the science has had a chance to mature and develop, and its effects on society better determined.").

[283] *See supra* notes 5, 51–58 and accompanying text.

[284] Such appears to be the solution in the proposed Stop Online Piracy Act, H.R. 3261, 112th Cong., § 102(c)(4)(A)(ii) (2011).

[285] In theory, at least, cases could exist in which changing an IP address could be viewed as an act of misrepresentation. *See, e.g.*, Lanham Act § 43(a), 15 U.S.C. § 1125(a) (2006) (misrepresentation of the origin of goods).

disclosure obligation that he would have to fulfill by always presenting himself to the outside world with his true IP address.

The change from IPv4 to IPv6 may support the idea of non-changeability of IP addresses. If one of the virtues of IPv6 is the ability to identify a particular device by its IP address, allowing users to change the IP addresses of their devices, even if only temporarily, would render the virtue worthless. Experts have promised that having IP addresses permanently assigned or embedded in various devices will be an advance that will spur further innovation in the online world because new applications may thereafter be developed to target specific devices connected to the Internet, and these devices will no longer be limited to computers or cell phones but will include devices such as cars, refrigerators, washing machines and other appliances.[286] Allowing cybertravel would hinder this development because applications could not rely on the user leaving the fixed IP address of a device unaltered.

In addition to being inconsistent with the interests of the parties aligned in support of IPv6, cybertravel also appears to be inconsistent with the desires of governments and the private sector to erect borders on the Internet. In spite of the zeal of true Internet enthusiasts to remain faithful to the original concept of the borderless network,[287] there are reasons why both governments and the private sector need a territorial partitioning of the Internet. Use of geolocation tools by website operators appears to be a reasonable method of erecting borders on the network;[288] however, the functioning of these tools can be undermined by cybertravel, which evades the tools and defeats the partitioning. Outlawing cybertravel seems to be a logical answer in support of the border-building process.

---

[286] *See, e.g.*, ICANN IPv6 News Conference: Miami, Fl., YOUTUBE (Feb. 3, 2011), http://www.youtube.com/watch?v=gveJs6YRYXU.

[287] *See supra* Part I.

[288] *See id.*

2. Cybertravel and the Right to Obscure One's Location[289]

The ability to assign permanent IP addresses to every device connected to the Internet, and the ability to attribute acts on the Internet to those devices and possibly to particular persons, raises serious privacy concerns.[290] This possibility explains an increasing interest, or even determination, among Internet users for options to change their IP addresses as a way of maintaining their privacy on the Internet. Indeed, services already exist that offer a simple way to obscure information about users' Internet connections by altering users' IP addresses.[291] These anonymizing services do not fit the definition of cybertravel because users do not necessarily use the services to evade geolocation to "travel" to another country; users seeking anonymization often want only to obscure their own IP address but do not care about the location of the replacement IP address.[292]

It might appear that the debate about the availability of anonymous Internet browsing relates to the future of cybertravel;[293] however, there is not necessarily a link between the legality of anonymization and the legality of cybertravel. The law may permit a change of IP address for the purposes of anonymization, yet require that the replacement IP address also be located in the jurisdiction of the user's physical location. This approach would achieve a certain level of anonymization that might be sufficient for many purposes,[294] and yet maintain the desired localization specificity of the IP address. The localization might not be detailed enough to bring the user localized

[289] I am indebted for this term to Megan M. Carpenter, Associate Professor of Law at Texas Wesleyan School of Law, who proposed its use in this context.

[290] If you were concerned about someone hacking into your computer you might decide that having someone hack into the contents of your refrigerator would be worse.

[291] *See supra* Part III (discussing examples of such concerns).

[292] *See id.*

[293] *See, e.g.*, Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1455–60 (2009) (discussing anonymization on the Internet).

[294] Anonymization in the same jurisdiction might not, in fact, always be sufficient–for example, if the jurisdiction is too small or has an insufficient number of Internet users with the same characteristics, identification of the particular user might be possible. Similarly, anonymization within the same jurisdiction will not work if the desire for anonymization is combined with a need to cybertravel.

information about restaurants, for example, but would be sufficiently detailed to allow website operators to detect the jurisdiction from which the user is connecting and adjust the accessibility of content accordingly. This solution would allow users a certain degree of anonymization but give them no ability to obscure their location to the point of avoiding compliance with territorially-defined laws and regulations.

Similarly, legalization of cybertravel does not automatically dictate a legalization of anonymization; depending on the structure of legal cybertravel, legalization of anonymization might be unnecessary and also undesirable. For instance, legal cybertravel might be conditioned upon the use of a digital passport that would identify not only the user's location or domicile but also the user's identity or account;[295] such a condition would permit cybertravel but require that the user maintain accurate information about his or her identity. This solution would allow cybertravel but defeat anonymization; users would be able to obscure their current location if, for instance, the digital passport required information about the user's domicile or residence but not the user's current location.

If the future of the Internet includes permanently assigned IP addresses, anonymous Internet speech may have to be safeguarded by means other than the obscuring of one's IP address, and alternative means are likely to require careful attention to the protection of privacy.[296] It is possible that privacy law could develop before any policy decisions are made concerning anonymization or cybertravel, and some experts will undoubtedly argue that as privacy protection becomes stronger for IP addresses, the arguments in favor of allowing users to change their IP addresses should yield.[297] Some experts may present this outcome

[295] *See infra* Part IV.C for a discussion of the impact of selecting the domicile instead of the current location.

[296] There will be someone in the process—some other "anonymizer"—who will know the IP address of the Internet user; therefore, privacy rules will have to protect the user from having this information disclosed.

[297] On the current difficulties of defining IP addresses as personal data or personally identifiable data see the following recent decisions: Bundesgericht [BGer] [Federal

as a necessary compromise: the law will protect a user's personally identifiable information, but the user will be expected to keep it personally identifiable. Although information subject to privacy protection must lead to the identification of a particular person (by definition), there seems to be no link between providing protection to such information and requiring that the particular person not change the information. The result of the debate may impact the design of cybertravel but should not be dispositive of the question of whether cybertravel should be legal or not; the answers to the questions about cybertravel and anonymization should not be mutually dependent.

3. Cybertravel as an Equivalent to Physical Travel

Because the developments outlined earlier appear to dictate that cybertravel be illegal in the future, it is difficult to find an argument for allowing cybertravel. One attempt is to analogize cybertravel to physical travel and claim an equivalent right to travel in cyberspace. If cybertravel is considered equivalent to physical travel, it can be argued that cybertravel should be permissible in some form and enjoy the same protections that physical travel—and in particular international travel—does.

The right to travel internationally has been recognized in the United States as a constitutional right,[298] and is implied as a human right in international human rights treaties.[299] In the 1958 case

Supreme Court] Sept. 8, 2010, 136 ENTSCHEIDUNGEN DES SCHWEIZERISCHEN BUNDESGERICHTS [BGE] II 508 (Switz.). ("It is impossible to determine in the abstract whether IP addresses [particularly dynamically assigned addresses] are personal data." *Id.*); Media C.A.T. Ltd. v. Malcolm Adams et al., [2011] EWPCC (En.) 6, [91]. *See also* Case C-70/10, Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=763036; *see generally* Joshua J. McIntyre, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected As Personally Identifiable Information*, 60 DEPAUL L. REV. 895 (2011).

[298] *See supra* note 10 and accompanying text; *see also* Timothy Zick, *The First Amendment in Trans-Border Perspective: Toward a More Cosmopolitan Orientation*, 52 B. C. L. R. 941, 954 (2011).

[299] Universal Declaration of Human Rights, Dec. 10 1948, G.A. Res. 217A U.N. GAOR, 3d Sess., 67th plen. mtg., U.N. Doc. A/810, art. 13(2) (1948) (includes "the right

*Kent v. Dulles*,[300] the Supreme Court of the United States discussed the constitutional right to travel internationally and explained the underpinnings of that right, surveyed the roots of the right in U.S. history and traditions,[301] and quoted Zechariah Chafee on social values associated with the freedom of movement.[302] Although some of the values cited in *Kent v. Dulles* are not pertinent to the present discussion of cybertravel (values of allowing families to reunite, persons to work in other countries),[303] others, such as educational values and the values of learning different viewpoints, are very relevant.[304] "In many different ways," the Supreme Court quoted Chafee, "direct contact with other countries contributes to sounder decisions at home."[305] It would seem that cybertravel is as much associated with these values as physical travel is.[306]

Even if, by analogy with physical travel, the right to travel internationally is extended to cybertravel, the right to cybertravel would be subject to limitation through governmental regulation analogous to the regulation that is applicable to physical travel. In the United States the right to travel internationally is subject to rational basis scrutiny, which allows the government to use reasonable means to limit the right as long as the limitation is

to leave any country, including his own, and to return to his country"); Protocol to the European Convention on Human Rights, Strasbourg, September 16, 1963, art. 2(2) (includes the freedom "to leave any country, including his own"); International Covenant on Civil and Political Rights, art. 12(2) (includes a provision that "[e]veryone shall be free to leave any country, including his own"); American Convention for Human Rights, Opened for Signature Nov. 22, 1969, Ch II, art. 22(2) (provides that "every person has the right to leave any country freely, including his own").

300 357 U.S. 116 (1958).

301 *Id*. at 125–26.

302 *Id.* at 126–27 (quoting ZECHARIAH CHAFEE, THREE HUMAN RIGHTS IN THE CONSTITUTION OF 1787 195–96 (Univ. of Kansas Press 1956)).

303 *Id.* (quoting ZECHARIAH CHAFEE, THREE HUMAN RIGHTS IN THE CONSTITUTION OF 1787 195–96 (Univ. of Kansas Press 1956)). In some contexts the right to be allowed to work in another country could require the right to cybertravel.

304 *Id.* (quoting ZECHARIAH CHAFEE, THREE HUMAN RIGHTS IN THE CONSTITUTION OF 1787 195–96 (Univ. of Kansas Press 1956)).

305 *Id.* at 127 (quoting ZECHARIAH CHAFEE, THREE HUMAN RIGHTS IN THE CONSTITUTION OF 1787 195–96 (Univ. of Kansas Press 1956)).

306 *But cf.* Zick, *supra* note 298, at 1004 (noting that the decisions of the U.S. Supreme Court that followed *Kent v. Dulles* "effectively neutered any First Amendment liberty to travel abroad for purposes of inquiry and information-gathering").

rationally related to a legitimate governmental interest.[307] Similarly, international treaties on human rights recognize that the right to travel across national borders may be limited.[308] For instance, the 1966 International Covenant on Civil and Political Rights, to which the United States has been a party since 1977 and which it ratified in 1992, allows restrictions of the right as long as the restrictions "are provided by law, are necessary to protect national security, public order (ordre public), public health or morals or the rights and freedoms of others, and are consistent with the other rights recognized in the . . . Covenant."[309] One of the generally accepted restrictions is the requirement that persons traveling across national borders carry passports that identify them and thereby allow countries to monitor the movement of persons. Indeed, it could be foreseen that in the digital environment countries could impose a similar requirement for cybertravel.

Some might argue that there is an even stronger argument for the protection of cybertravel—the right of access to information.[310] International treaties, including treaties to which the United States is a party, define the right of freedom of expression to include the right to access information from wherever it may be located. For example, Article 19 of the Universal Declaration of Human Rights protects the right "to *seek*, *receive* and impart information and ideas through any media and *regardless of frontiers*."[311] In the United States some commentators have advocated that the right to

[307] *See* Califano v. Aznavorian, 439 U.S. 170, 178 (1978). This is different from domestic travel, which is protected by a higher level of scrutiny. *Id.* at 176–78.

[308] But the 1948 Universal Declaration of Human Rights does not include a provision on limitations of the right. Universal Declaration of Human Rights, G.A. Res 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).

[309] International Covenant on Civil and Political Rights art. 12(3), Dec. 16, 1966, 99 U.N.T.S. 171; *see also* Protocol to the European Convention on Human Rights art. 2(3), Sept. 16, 1963, 213 U.N.T.S. 221; American Convention on Human Rights art. 22(3), Nov. 22, 1969, 1144 U.N.T.S. 143.

[310] On the potential overlap between the right to travel and the right to free speech see Zick, *supra* note 298, at 954–57, 985–86, 1004–12.

[311] Universal Declaration of Human Rights art. 19, G.A. Res 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948) (emphasis added). *See infra* note 320 for other treaties that protect the right to seek, receive and impart information without territorial limitations.

travel internationally be derived from the free speech protection of the First Amendment rather than from the Due Process Clause because of the values encompassed by international travel.[312] Advocates of this view could use cybertravel to help persuade countries to acknowledge this link between the right to international travel and the right to free speech; to many, the link may be more relevant in the context of cybertravel than physical travel.[313] If countries refuse to link the concepts, of course, equating cybertravel to physical travel would not improve cybertravel's chances of benefitting from the protection of access to information.

Any attempt to extend the rights of international travel or access to information to cyberspace would certainly not be the first attempt to assert constitutional and human rights in cyberspace.[314] The first constitutional right to receive attention in the context of the Internet was the right to free speech; users have asserted this right when faced with limitations on Internet speech imposed by other countries. The *Yahoo!*[315] and *Viewfinder*[316] cases are examples of cases in which U.S. courts have denied recognition and enforcement of foreign judgments because of the significant

---

[312] Zick, *supra* note 298, at 1005, 1008; *see also supra* INTRODUCTION (discussing the values associated with travel).

[313] Zick is concerned that the focus on protecting free speech on the Internet will distract attention from the need to protect international travel:

> [I]t may be tempting to reason that because speech can transcend territorial borders via the Internet, there is less need for a fundamental right of cross-border movement. But even in the digital era, freedom of speech and other First Amendment liberties still depend upon rights of cross-border movement and trans-border information-gathering. . . . [I]t remains important that we have a constitutional foundation for cross-border movement and intermingling.

Zick, *supra* note 298, at 1004–05.

Cybertravel is an activity on the Internet that could provide additional support for the right to travel internationally.

[314] *E.g.*, *Charter of Human Rights and Principles for the Internet, Version 1.1 for Consultation*, INTERNET RIGHTS & PRINCIPLES COAL., http://www.freedomofexpression.org.uk/files/DRAFTVersion1.1%283%29.pdf (last visited Nov. 19, 2011).

[315] Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001), *rev'd en banc*, 433 F.3d 1199 (9th Cir. 2006).

[316] Sarl Louis Feraud Intl. v. Viewfinder, Inc., 489 F.3d 474 (2d Cir. 2007).

public policy embedded in the U.S. constitutional guarantee of free speech. In line with these cases and other cases involving foreign libel judgments and speech on the Internet, the 2010 SPEECH Act ensures that no foreign defamation judgments will be recognized in the United States unless they comport with U.S. standards of free speech.[317]

One problem in asserting the right to free speech on the Internet is that the functioning of the Internet depends on non-state actors, and only when constitutional rights or human rights involve governmental action that must be effectuated on the Internet by non-state actors (such as recognition and enforcement of a foreign judgment, or content filtering mandated by the government) will an assertion of constitutional rights on the Internet be possible.[318] Given the importance of the Internet, it is not surprising that experts such as Christoph B. Graber are calling for an extension of the rights to bind private actors on the Internet;[319] the actors to be bound by the rights should be the providers of critical Internet infrastructure, such as Internet service providers, intermediaries, and others who are providers of web services that are unique and indispensible to the usability of the Internet. Graber gives an example of preemptive filtering that demonstrates the risk of serious intrusions into the right to "communicative freedom," which in his definition includes not only the right to free speech, but also the "passive" aspect of the right, which is the right of access to information—a right that is embedded in international human rights treaties.[320] The filtering in Graber's example is

[317] Securing and Protecting our Enduring and Established Constitutional Heritage (SPEECH) Act, 28 U.S.C. §§ 4101–05 (2010).

[318] On "Constitutional Rights in the Private Sphere of the Internet" from a comparative perspective see Graber, *supra* note 42, at 17–20.

[319] *See generally* Graber, *supra* note 42; *see also* Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 988 (2008) ("[I]f individuals' speech should not be attributed to intermediaries when it is unlawful, we should at least consider ways in which intermediaries could be deterred from interfering with it when it is lawful."). Rebecca Tushnet argues that "if we limit intermediary responsibility . . . we should also limit intermediary power to control speech." *Id.* at 1009.

[320] The "right to freedom of opinion and expression . . . includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas

conducted by intermediaries who block user access to peer-to-peer networking sites or other websites with potentially infringing content, thereby preemptively censoring speech that might not be infringing at all.[321] Such censorship, if conducted by a government, would be contrary to free speech protections and subject to legal recourse; however, no recourse is available to users when the filtering is conducted by private actors.[322]

Users expect Internet service providers to comply with constitutional and human rights, and as the Internet has changed from being solely a means of communication to a medium for many other activities, such as trade and entertainment, the expectations for constitutional and human rights on the Internet have expanded beyond free speech. For example, if users have built their business models on selling merchandise on eBay, and eBay at some point no longer allows them to sell on eBay, this has a drastic impact on their livelihood. Although an initial

through any media and regardless of frontiers." Universal Declaration of Human Rights art. 19, G.A. Res 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948). The right to freedom of expression "shall include freedom to *seek, receive* and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." International Covenant on Civil and Political Rights art. 19(2), Dec. 16, 1966, 99 U.N.T.S. 171. (emphasis added). For permissible limitations on the right see *id.* at art. 19(3). The right to freedom of expression "shall include freedom to hold opinions and to *receive* and impart information and ideas without interference by public authority and regardless of frontiers." European Convention on Human Rights art. 10(1), Nov. 4, 1950, 213 U.N.T.S. 221 (emphasis added). For permissible limitations on the right see *id.* at art. 10(2); *see also* American Convention on Human Rights art. 13, Nov. 22, 1969, 1144 U.N.T.S. 143; Recommendation CM/Rec(2008)6 of the Committee of Ministers of the Council of Europe to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, Mar. 26, 2008.

[321] Graber, *supra* note 42, at 10. For a similar argument concerning a "prior restraint by proxy," see Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171 (2010). Seltzer notes that the actions of service providers in her example are mandated by law and states that "[g]overnment cannot insulate itself from responsibility for this abridgment of free speech by routing its influence through third-party service providers." *Id.* at 190.

[322] *See also* Peter K. Yu, *The Graduated Response*, 62 FLA. L.R. 1373, 1398 (2010) (in the context of takedowns by service providers based on DMCA notifications and the graduated response approach).

incarnation of the problem of Internet users' expectations clashing with Internet service providers' actions was small merchants demanding continuing access to eBay,[323] the subsequent debate about network neutrality shows that the problem of accessibility has entered a new and more critical stage.[324] Not only is the right to free speech at stake, but other rights are as well. For instance, following the unrest in Egypt in January and February 2011, Mohamed ElBaradei, the leading opposition figure, was quoted as observing that prior to the shutdown of the Internet by the government, the Internet had provided the right to freedom of association that was missing *de facto* on the ground.[325] Indeed, it is an exercise of this constitutional right that today's Internet users expect private actors such as Twitter or Facebook to facilitate. It is understandable that people relying on the infrastructure of the Internet will search for constitutional protections for their access to the infrastructure.[326]

Constitutional and human rights may in the future shield Internet users not only from governmental intrusion, but also from certain acts by Internet service providers and other providers of critical infrastructure—regardless of whether such acts result from indirect governmental intervention or voluntary decisions by providers.[327] The right to travel should enjoy parity with the right to free speech, the right to free assembly, the right to access to

---

[323] "PowerSellers" on eBay objected to eBay's practice of denying them access to the auction website based on repeated complaints filed against them under the DMCA, 17 U.S.C. §512(c)(3) (2006). For a discussion of the problem, see Trimble, *Enemy Ground*, *supra* note 173, at 808–09.

[324] Cecilia Kang, *FCC Approves Net-Neutrality Rules; Criticism Is Immediate*, WASH. POST (Dec. 22, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/12/21/AR2010122106110.html.

[325] Interview by NPR with Laban Coblentz, a speechwriter for Mohamed ElBaradei (Feb. 7, 2011), *available at* http://thestory.org/archive/the_story_020711_full_show.mp3/view.

[326] Although private actors who furnish critical infrastructure may resist any new legal obligations that countries may attempt to impose upon them, the actors may have no choice other than to accept the additional obligations: if a critical part of the Internet is in the hands of one or a small number of private actors, countries will have a limited ability—short of nationalizing that part of the Internet—to protect constitutional rights in cyberspace.

[327] *See* Interview by NPR with Laban Coblentz, *supra* note 325.

information, and other recognized constitutional and human rights that should be fully implemented on the Internet.

### *C. Can Cybertravel be Legal?*

If we accept the premise that cybertravel, or the capability of a user to evade geolocation and use the Internet as if he were located in a location other than where he is physically located, is socially valuable and worth permitting in some form, the question turns to the conditions under which cybertravel could be legal. As explained earlier, the existence of this capability does not depend on permitting anonymity on the Internet;[328] anonymization and cybertravel need not go hand in hand.

Thinking about the possible future of cybertravel requires considering all of the various policies and business motives that lead website operators to limit access to their content on the Internet.[329] First, website operators design content limitations to enhance user convenience by localizing accessible content, for example by showing advertisements for local businesses. Second, website operators may have contractual obligations with content providers, for example to limit access to video programs that a provider has licensed only for certain countries or regions.[330] Third, the operators may limit access to content to comply with laws that prohibit certain types of content in certain countries, for example by blocking gambling when it is outlawed by some countries. Prohibitions may also apply, however, for less-maligned content that may be made inaccessible because of countries' legal requirements—for instance, countries' consumer protection laws may require certain products to be offered only if they have been certified for use in the country.[331] Fourth, website operators may decide voluntarily to limit access to content to avoid being exposed to personal jurisdiction and liability in certain countries where they wish to avoid litigation, taxes, regulation or some other type of obligation. Finally, website operators may

328 *See supra* Part IV.B.2.
329 *See supra* Part II.A (discussing the various reasons).
330 *Id.*
331 *Id.*

implement access limitations for security reasons; for example, a bank will not allow a user from outside the account holder's country of residence to log into the account holder's account because the bank assumes that such a login is a fraudulent attempt to access the account.

The first type of restriction—content localized for advertising or for user convenience—should cause the least difficulty. There should be no reason for prohibiting users from viewing this type of content as if they were sitting in another country. In fact, website operators such as Google and Lufthansa offer links to allow users to switch easily among different country versions.[332] This switching may not be completely without cost to the website operator, however; if users regularly escape the "convenience" of localized content and use other country versions in lieu of their own local versions, it may diminish website operators' advertising revenues because they lose some of the advantage that a partitioned cyberspace provides in allowing them to charge premium advertising rates for advertisements that target local consumers.

Cybertravel that is used to evade the other types of access limitations listed above is problematic. It is unrealistic to expect countries to allow users connecting to the Internet from their territory to bypass any prohibitions against certain content or activities by cybertraveling to another country where such content or activities are expressly or implicitly permitted. Allowing cybertravel for these purposes would defeat the public policies behind the prohibitions and undermine national sovereignty. Similarly, it is difficult to defend cybertravel that is used for the purpose of bypassing geolocation tools employed by website operators who are complying with contractual obligations, seeking to avoid personal jurisdiction and liability, or protecting themselves and others against criminal activities. The question is whether there is a way to permit cybertravel when it is conducted to avoid these types of limitations, but the conduct has a legitimate goal, such as accessing one's own bank account from a foreign

[332] *Id.*

country. The method of cybertravel is not important, because the tools for its implementation will change;[333] what is important is that travel to another portion of cyberspace be possible.[334]

There are three perspectives from which possible solutions for the future of cybertravel will arise: legal, technological and business. As has been shown by other examples in the Internet environment, a combination of solutions from all three perspectives seems most likely to succeed. For example, laws that prohibit copyright infringement have not stopped online music piracy, and neither have filters that have been imposed by Internet service providers or automatic warnings that are generated by college campus service providers. Although these measures and laws addressing piracy have probably slowed online music and film piracy, the solutions had to be assisted by business solutions, such as iTunes and Netflix, to offer a legal and viable alternative to piracy.

As discussed earlier in section IV.A, a number of legal doctrines cover issues potentially associated with cybertravel; however, because these doctrines were neither created for nor shaped with cybertravel in mind, courts will be required to determine the extent to which the doctrines may make illegal all or some instances of cybertravel.[335] Whatever the status of cybertravel will be, it will be beneficial to clarify the applicability of existing laws to cybertravel and possibly draft specific regulations to govern cybertravel further. If IPv6 makes IPv4 obsolete and a transition actually occurs to permanently assigned or embedded IP addresses, the transition could provide momentum for the creation of cybertravel-specific legislation, and perhaps even for an agreement on a legislative solution at the international level.

Within some permitted extent, cybertravel, as an equivalent to physical international travel, could be subject to reasonable

333 *See supra* Part III (explaining the functioning of various cybertravel tools).

334 *See supra* Part I (explaining the "borderlessness" of the Internet and the impetus for partitioning of the Internet).

335 *See supra* Part IV.A.

limitations. Traditionally, the obligation to carry a passport is considered one such limitation, and a digital passport could serve this purpose for cybertravel. The passport could either be a virtual equivalent to a physical passport and carry the same personally identifiable data of the holder/Internet user, or be a document with only limited information, such as the user's location. The location identified in either type of passport could be either the current physical location of the user or the place of residence or domicile of the user, depending on the criterion that was set as the factor determining the accessibility of the Internet content.

Although intuition seems to dictate the selection of the user's current physical location as the determining factor, the other option—place of residence or domicile—should not be summarily excluded. The prevailing principle of territoriality of law suggests that current physical location be the correct solution; under the principle, laws apply territorially, or alternatively stated, the prescriptive jurisdiction of a country extends only to the country's borders—and outside its borders only to the extent that the country's jurisdiction covers acts that have effects within its borders. Another principle, the principle of personality of law, exists as well, but with less applicability because the principle of territoriality of law applies to the vast majority of the legislative activities of a country. The use of residence or domicile as the determinative factor for access to Internet content would present a remarkable opportunity to introduce the principle of personality of law for activity on the Internet. Under this principle countries legislate for their own nationals and permanent residents and the laws follow those persons wherever they travel. An analysis of the issues surrounding personality of law on the Internet is beyond the scope of this article and deserves a separate study, but is worth mentioning.

A law for digital passports cannot exist without a technological implementation. It is not difficult to imagine such a system if the IPv6-related vision of permanently assigned or embedded IP addresses that would identify specific devices (or even persons if the devices were embedded in human bodies) becomes a reality; the law could make it illegal to change or reroute an IP address because that act would be equivalent to forging a physical

passport. The digital passport would inform each website operator about the location of the user, or the user's residence or domicile, depending on the information in the passport.

Knowing exactly how many cybertravelers are connecting to a website and from what locations could assist intellectual property owners, for example, in the creation of tailored licensing schemes;[336] if information about cybertravelers were to include personal identifiers, the system could become what Paul Goldstein described in 1994 as the "celestial jukebox"[337]—a service that would allow on-demand access to copyrighted works from anywhere in the world for a fee.[338] The digital environment is perfectly equipped to implement this system;[339] in such a world, each user could access copyrighted works from anywhere in the world and be charged only for works that the user accessed. This is where a technological solution would prompt the need for a business solution.

What hampers progress towards a "celestial jukebox" are the significant transaction costs associated with the identification and location of right holders and the negotiation of licenses with multiple right holders. The magnitude of these costs must be addressed in order for global licensing to be feasible, and there are initiatives being developed in this area to pave the way for this type of solution;[340] for example, experts have proposed that the World Intellectual Property Organization create and administer an international repertoire database,[341] and other experts are exploring

---

[336] *See* Loesing et al., *supra* note 156, at 205 ("There are estimated to be hundreds of thousands [of] Tor users every day routing their data through the Tor network.").

[337] PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY: FROM GUTENBERG TO THE CELESTIAL JUKEBOX 28–29 (1994). Paul Goldstein claims no credit for the celestial jukebox metaphor.

[338] *See id.*

[339] *See id.*

[340] *See* Jane C. Ginsburg, *International Issues: Which Country's Law Applies When Works Are Made Available Over the Internet?*, 34 COLUM. J.L. & ARTS 49, 53 (2010) ("[T]he practice . . . of extended collective licenses, albeit not yet E.U. wide, is growing.").

[341] Kaitlin Mara & William New, *Should WIPO Lead Creation of a Global Repertoire Database?*, INTELL. PROP. WATCH (Nov. 22, 2010), http://www.ip-watch.org/weblog/2010/11/22/should-wipo-lead-creation-of-global-database-of-music-repertoire/. The

possibilities for cross-border collective management of rights in the digital environment.[342]

Even without a celestial jukebox solution that would cover all works globally, and even without digital passports, there is clearly space for smaller-scale business solutions to meet the challenges of cybertravel. If content is limited because of the contractual obligations of website operators, cybertravel could be enabled by global or regional licensing schemes that would allow operators to offer certain content either worldwide or in selected countries.[343] Instead of paying cybertravel providers to facilitate cybertravel, users would pay for access directly to website operators, who would then bear any licensing costs and any other costs associated with the content, such as a public television licensing fee.

Of course, these solutions are directed only toward access to content that is restricted because of contractual limitations; any content that is illegal in a country will continue to be inaccessible to users accessing the Internet from that country, and potentially to nationals or permanent residents of that country even when they are temporarily present in another country, if digital passports are used. For certain types of content—and the instances of these types of content are likely to be limited—countries may reconsider the legal status of content in light of the possibilities afforded by digital passports. For example, some countries might reconsider

Court of Justice of the European Union has undertaken what may be interpreted as a push for pan-European licensing. *See* Cases C-403/08 & C-429/08, Football Ass'n Premier League Ltd. v. QC Leisure (Oct. 4, 2011), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=110361&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=27863.

342 *E.g.*, Torben Toft, *Collective Rights Management in the Online World: A Review of Recent Commission Initiatives*, EUR. COMM'N, DG COMPETITION, at 14 (June 8, 2006), http://ec.europa.eu/competition/speeches/text/sp2006_008_en.pdf; *see generally* Brian R. Day, *Collective Management of Music Copyright in the Digital Age: The Online Clearinghouse*, 18 TEX. INTELL. PROP. L.J. 195 (2010); *A Digital Agenda for Europe: Commc'n from the Comm'n to the Eur. Parl., the Council, the Eur. Econ. and Social Comm. and the Comm. of the Regions*, COM(2010) 245 final (Aug. 26, 2010).

343 *See supra* Part IV.A.1 (providing an example of the BBC preparing to launch its TV shows for viewing by users accessing the BBC website from outside the United Kingdom).

their stance on online gambling if they have the ability to tax users located in their country who use foreign online gambling sites.

The solutions also fail to address cases in which access to content is limited by a website operator's or content provider's choice; these cases arise because of issues of jurisdiction, taxation or online security. When website operators or content providers decide *sua sponte* to restrict their content to certain viewers, users have minimal recourse; only in rare circumstances will a government direct private entities to make content more widely available than it already is. Here a system of digital passports could prove useful; for example, if access to content were based on a user's permanent residence, content could be made available to a qualified user while he was temporarily located in another country, without exposing the website operator to jurisdiction or taxation in that country.

Finally, knowledge of the numbers and physical locations of cybertravelers could make possible not only sophisticated licensing arrangements but also agreements—either private (meaning between individual content providers and website operators) or international (meaning among countries)—as to an acceptable level of free spillover. In the physical world, it is accepted that some content limited to a certain country will be available to those who travel to that country. For example, when distribution rights under copyright are licensed for one country, it is understood that some of the copyrighted works will land in the hands of persons who are present in the country only temporarily and those persons may carry the work with them to other countries; laws provide exceptions for individual users to do this because it is considered natural spillover.[344] Exceptions for a similar reasonable spillover could be permitted for cybertravel. However, without information about the extent of cybertravel, it is impossible to find arguments

[344] *E.g.*, Agreement on Trade-Related Aspects of Intellectual Property Rights art. 60, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299; Council Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights, art. 3(2), 2003 OJ (L 196) 7, 9.

to support the exceptions for the spillover; a passport system would allow the collection of such information.

## CONCLUSION

This article presents a comprehensive analysis of cybertravel—the evasion by a user of geolocation that prevents the user from viewing certain Internet content from the user's physical location. By cybertraveling, the user can view the Internet as if the user were located in a country other than the country in which the user is physically located. The goal of the article is to explain what cybertravel is, why it exists, what purposes it serves, what its legal status is, what arguments exist for making it available in the future, and what solutions might be developed to allow users to cybertravel for legitimate purposes without undermining the evolution of the Internet. It seems clear that even though cybertravel will probably not survive in its current form, new technological and business solutions will preserve the concept and the law will complement these solutions.

The current importance of questions regarding the future of cybertravel is heightened by the desire of governments and the private sector to erect borders on the Internet to achieve compliance with territorially-defined regulation. This article assumes that this desire is shaping or will shape the future of the Internet, and that geolocation tools will play a major role in the future in light of user disfavor toward alternative types of access controls: user hardware filtering and Internet service provider filtering. However, it is possible that countries will adopt still other approaches to the problem of "missing borders." For example, courts could continue to use a low-technology approach to defining personal jurisdiction on the Internet,[345] thereby relieving website operators of the necessity of employing geolocation tools to comply with the laws of different countries. Or, instead of mandating Internet service provider filtering of

[345] *See supra* note 95 and accompanying text (discussing the low-technology approach to the determination of personal jurisdiction).

possibly prohibited content, countries could decide to implement detailed Internet traffic monitoring and aggressively identify and pursue users engaging in illegal activity in cases where countries cannot pursue website operators.

Although it is possible that the use of geolocation tools will not be the method of choice for the territorial partitioning of cyberspace in the future, it appears to be the preferred method at present. Partitioning through the use of geolocation tools enjoys a number of advantages when compared to other available methods,[346] and even if the alleged benefits of IPv6 are not fully utilized and IPv6 does not lead to permanently assigned or embedded IP addresses, geolocation tools can still function to achieve the goal of cyberspace partitioning that many Internet actors desire. However, for Internet partitioning to be truly effective the problem of cybertravel must be addressed; cybertravel frustrates the success of geolocation tools, making it difficult to determine or even estimate the effectiveness of these tools.[347]

The legal framework in which cybertravel operates is a patchwork of legal doctrines that were not formulated to regulate cybertravel, or even conceived with cybertravel in mind.[348] Whether the doctrines apply to cybertravel, and if so to what extent, are questions that courts will have to address. Copyright will probably be the area in which litigation will first arise, and the first issues targeted will be associated with making content available to audiences to whom the copyright holder did not intend to extend access. These disputes will emulate cases concerning place-shifting services that have arisen recently, such as litigation involving ManekiTV in Japan, TV Catch UP in the United Kingdom, and ivi and Justin.tv in the United States.[349] Cybertravel disputes will define the next generation of these cases.

---

346 *See supra* Part I, IV.B.3 (discussing the advantages and disadvantages of the methods of partitioning cyberspace).

347 *See supra* Part II.B (discussing the effectiveness of geolocation tools).

348 *See supra* Part IV.A (discussing the current legal status of cybertravel).

349 *See supra* Part Introduction, IV.A.2 (discussing the cases and their potential impact on cybertravel).

The extent to which cases concerning cybertravel will appear in courts, what the outcome of such cases might be, and whether or not any particular legal doctrines will be found to apply to cybertravel, are questions that merit a thorough analysis. The undeniable value in being able to view the Internet as if one were located in another country, and the legitimate reasons why users want or need to cybertravel warrant the consideration of options for legal cybertravel. This article suggests that cybertravel should be analogized to physical travel, and the benefits that society will enjoy through cybertravel correspond in large measure to the benefits provided by physical travel.[350] Therefore, cybertravel should enjoy constitutionally protected rights.

Of course, cybertravel is free of the natural barriers that limit physical travel. As a result, a greater number of users can engage in cybertravel than in physical travel, and the volume and quality of reproduction of the content that cybertravelers can obtain will usually be much higher than that of the content that physical travelers may carry back to their country.[351] This means that content spillover that may be negligible in cases of physical travel can in the case of cybertravel almost instantaneously exceed what anyone might consider reasonable spillover.[352] For example, while the number of foreign visitors who buy a book in one country and travel home with it may number in the thousands, the number of foreign users cybertraveling to access a television show may be in the millions. One problem for cybertravel is that there are no data available to suggest the size of the cybertravel phenomenon, and it is difficult to formulate arguments in response to those who claim that cybertravel is a significant problem unless some data are collected to support a claim that cybertravel, like physical travel, leads to only negligible spillover.

---

350 *See supra* Part IV.B.3 (discussing the arguments for equating cybertravel to physical travel).

351 High volume data storage allows for a similar volume of data to be transported physically and with the same potential reproduction quality. However, cybertravel remains a faster and easier mode for transporting data.

352 *See supra* Part IV.C (discussing a reasonable spillover associated with physical travel).

Even if it can be proven that cybertravel does not currently pose any significant threat to right holders, website operators, and countries' efforts to limit access to certain content, cybertravel technology is rapidly changing and new simplified tools permit more users, even ones with extremely limited technical skills, to cybertravel. More Internet users will also be prompted to cybertravel because of the increased use of geolocation tools by website operators. The legal, technological, and business solutions will need to address the practice of cybertravel and shape an environment in which legal cybertravel—cybertravel for legitimate purposes—will be available.

This article explores one answer to cybertravel—a system of digital passports that would either identify specific users or provide a minimum of information about a user's location, domicile, or permanent residence. A technological solution supported by an appropriate legal framework and enhanced by sophisticated business solutions could solve the problem of cybertravel and increase the opportunities that the partitioned Internet offers. This system would need to be supported by a strict data protection structure that would impose both legal and technical requirements on Internet actors. Although increased data protection requirements may face strong resistance from some Internet actors today, strict data protection must be integrated into the cyberspace future.